

503 P13 36WOOD .1

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2002-84271

(P 2 0 0 2 - 8 4 2 7 1 A)

(43) 公開日 平成14年3月22日 (2002.3.22)

(51) Int. Cl. <sup>7</sup>

識別記号

F I

テーマコード (参考)

H04L 9/08

G11B 20/10

H 5D044

G11B 20/10

H04L 9/00

601

D 5J104

審査請求 未請求 請求項の数40 O L (全56頁)

(21) 出願番号 特願2000-270919 (P 2000-270919)

(22) 出願日 平成12年9月7日 (2000.9.7)

(71) 出願人 000002185

ソニー株式会社

東京都品川区北品川6丁目7番35号

(72) 発明者 浅野 智之

東京都品川区北品川6丁目7番35号 ソニー株式会社内

(72) 発明者 大澤 義知

東京都品川区北品川6丁目7番35号 ソニー株式会社内

(74) 代理人 100101801

弁理士 山田 英治 (外2名)

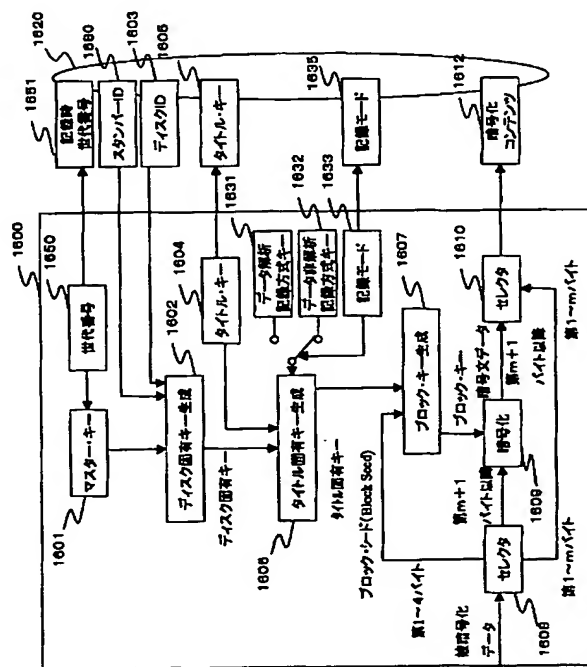
最終頁に続く

(54) 【発明の名称】 情報記録装置、情報再生装置、情報記録方法、情報再生方法、および情報記録媒体、並びにプログラム提供媒体

(57) 【要約】

【課題】 不正なコンテンツの利用を効果的に排除可能とした情報記録、再生装置を提供する。

【解決手段】 記録媒体に、あらかじめその書き込み/読み出し方法が解析困難な、特殊の読み出し方法でのみ読み取り可能な秘密情報を格納し、記録媒体に対する音楽データ、画像データ等のコンテンツの記録あるいは再生を行う際のコンテンツ暗号化あるいは復号処理用暗号鍵に、上記秘密情報を作用させる。秘密情報は、例えばスタンパーIDであり、秘密情報としてのスタンパーIDと、ツリー構造の鍵配布構成により配布されるマスターキー、メディアキー等と共にコンテンツの暗号処理鍵の生成を行なう。従って、秘密情報についての特殊な読み取り方法を実行可能で、かつツリー構造の鍵配布構成により鍵の配布された正当デバイスでのみコンテンツの利用が可能となる。



ブを含み、

前記暗号化キー生成用データは、複数の異なる情報記録装置をリーフとし、各分岐をノードとして各ノード、リーフに固有のキーを設定した階層ツリー構造のノードキーを下位階層のノードキーまたはリーフキーの少なくともいずれかを含むキーにより暗号化した有効化キブロック (EKB) によって更新可能なデータであることを特徴とする請求項 1 9 に記載の情報記録方法。

【請求項 2 3】前記暗号化キー生成用データは、複数の情報記録装置において共通なマスターキー、または特定の記録媒体に固有のメディアキーのいずれかであることを特徴とする請求項 2 2 に記載の情報記録方法。

【請求項 2 4】前記暗号化キー生成用データは、更新情報としての世代番号が対応付けられた構成であり、前記暗号処理ステップは、前記記録媒体に対する暗号化データ格納時に、使用した前記暗号化キー生成用データの世代番号を記録時世代番号として前記記録媒体に格納するステップを含むことを特徴とする請求項 2 2 に記載の情報記録方法。

【請求項 2 5】前記情報記録方法は、さらに、トランスポートパケットから成るトランスポートストリームを構成する各パケットに受信時刻情報 (ATS) を付加するトランスポート・ストリーム処理ステップを有し、前記暗号処理ステップは、前記受信時刻情報 (ATS) の付加された 1 以上のパケットからなるブロックデータに対する暗号化キーとしてブロックキーを生成するステップを含み、前記記録媒体に対する格納データの暗号処理においては、前記秘密情報と、前記暗号化キー生成用データと前記受信時刻情報 (ATS) を含むブロックデータ固有の付加情報であるブロックシードとを含むデータに基づいて暗号化キーとしてのブロックキーを生成することを特徴とする請求項 2 2 に記載の情報記録方法。

【請求項 2 6】前記秘密情報復号処理ステップは、秘密情報を形成するビット列を 2 進数系列により擾乱して記録媒体に格納されたデータの復号処理を実行する復号処理ステップを含み、該復号処理ステップは、前記 2 進数系列を生成し、生成 2 進数系列と前記記録媒体からの再生信号との演算処理を実行して秘密情報の復号処理を実行することを特徴とする請求項 1 9 に記載の情報記録方法。

【請求項 2 7】前記秘密情報復号処理ステップは、秘密情報を構成する複数ビット単位に予め定められた規則に従って変換されて記録されたデータを記録媒体から読み取り、読み取りデータを再変換して秘密情報の復号処理を実行することを特徴とする請求項 1 9 に記載の情報記録方法。

【請求項 2 8】記録媒体から情報を再生する情報再生方

法において、

記録媒体に格納されたコンテンツデータの読み取り態様と異なる特殊なデータ読み取り処理を実行し、記録媒体に格納された秘密情報を読み取る秘密情報復号処理ステップと、

前記秘密情報復号処理ステップにおいて記憶媒体から読み取られ復号された秘密情報をキー生成用データとしてコンテンツ復号キーを生成し、該コンテンツ復号キーに基づいて記録媒体から読み取られるデータの復号処理を実行する復号処理ステップと、

を有することを特徴とする情報再生方法。

【請求項 2 9】前記秘密情報は、記録媒体の製造時に記録媒体に格納され、複数の記録媒体において共通なスタンパー ID、または個々の記録媒体に固有なディスク ID、コンテンツ毎に異なって設定するコンテンツ ID、あるいは暗号処理用のキーのいずれかのデータを含み、前記秘密情報復号処理ステップは、記録媒体から読み取られた秘密情報の復号処理を実行することを特徴とする請求項 2 8 に記載の情報再生方法。

【請求項 3 0】前記復号処理ステップは、前記秘密情報復号処理手段において読み取られた秘密情報を使用し、コンテンツ復号キーを生成するステップを含み、読み取られた秘密情報は情報記録装置外部からの読み取り可能な記憶手段への格納処理を行わず、前記暗号処理部内で実行されるコンテンツ復号キー生成処理においてのみ利用可能としたことを特徴とする請求項 2 8 に記載の情報再生方法。

【請求項 3 1】前記情報再生方法において、前記復号処理ステップは、前記秘密情報復号処理手段において読み取られた秘密情報と、情報再生装置に内蔵した復号キー生成用データに基づいて前記コンテンツ復号キーを生成するステップを含み、前記復号キー生成用データは、複数の異なる情報再生装置をリーフとし、各分岐をノードとして各ノード、リーフに固有のキーを設定した階層ツリー構造のノードキーを下位階層のノードキーまたはリーフキーの少なくともいずれかを含むキーにより暗号化した有効化キブロック (EKB) によって更新可能なデータであることを特徴とする請求項 2 8 に記載の情報再生方法。

【請求項 3 2】前記復号キー生成用データは、複数の情報再生装置において共通なマスターキー、または特定の記録媒体に固有のメディアキーのいずれかであることを特徴とする請求項 3 1 に記載の情報再生方法。

【請求項 3 3】前記復号キー生成用データは、更新情報としての世代番号が対応付けられた構成であり、前記復号処理ステップは、前記記録媒体からのデータ再生時に、使用した前記復号キー生成用データの世代番号を記録時世代番号として前記記録媒体に格納するステップを含むことを特徴とする

請求項 31 に記載の情報再生方法。

【請求項 34】前記情報再生方法は、さらに、  
トランスポートパケットから成るトランスポートストリームを構成する各パケットに受信時刻情報 (ATS) を付加するトランスポート・ストリーム処理ステップを有し、  
前記復号処理ステップは、  
前記受信時刻情報 (ATS) の付加された 1 以上のパケットからなるブロックデータに対する暗号化キーとしてブロックキーを生成するステップを含み、  
前記記録媒体からのデータの再生処理においては、前記秘密情報と、前記復号キー生成用データと前記受信時刻情報 (ATS) を含むブロックデータ固有の付加情報であるブロックシードとを含むデータに基づいて復号キーとしてのブロックキーを生成することを特徴とする請求項 31 に記載の情報再生方法。

【請求項 35】前記秘密情報復号処理ステップは、  
秘密情報を形成するビット列を 2 進数系列により擾乱して記録媒体に格納されたデータの復号処理を実行する復号処理ステップを含み、  
該復号処理ステップは、  
前記 2 進数系列を生成し、生成 2 進数系列と前記記録媒体からの再生信号との演算処理を実行して秘密情報の復号処理を実行することを特徴とする請求項 28 に記載の情報再生方法。

【請求項 36】前記秘密情報復号処理ステップは、  
秘密情報を構成する複数ビット単位に予め定められた規則に従って変換されて記録されたデータを記録媒体から読み取り、読み取りデータを再変換して秘密情報の復号処理を実行することを特徴とする請求項 28 に記載の情報再生方法。

【請求項 37】情報を記録可能な情報記録媒体であって、  
通常格納データの読み取り態様と異なる特殊なデータ読み取り処理を実行することによってのみ再生可能な秘密情報と、  
該秘密情報を適用して生成可能な暗号処理鍵により復号可能な暗号化コンテンツを格納したことを特徴とする情報記録媒体。

【請求項 38】前記秘密情報は、複数の記録媒体において共通なスタンパー ID、または個々の記録媒体に固有なディスク ID、コンテンツ毎に異なって設定するコンテンツ ID、あるいは暗号処理用のキーのいずれかのデータを含むことを特徴とする請求項 37 に記載の情報記録媒体。

【請求項 39】記録媒体に情報を記録する情報記録処理をコンピュータ・システム上で実行せしめるコンピュータ・プログラムを提供するプログラム提供媒体であって、前記コンピュータ・プログラムは、  
記録媒体に格納されたコンテンツデータの読み取り態様

と異なる特殊なデータ読み取り処理を実行し、記録媒体に格納された秘密情報を読み取る秘密情報復号処理ステップと、

前記秘密情報復号処理ステップにおいて記憶媒体から読み取られ復号された秘密情報をキー生成用データとしてコンテンツ暗号化キーを生成し、該コンテンツ暗号化キーに基づいて記録媒体に格納するデータの暗号処理を実行する暗号処理ステップと、  
を有することを特徴とするプログラム提供媒体。

10 【請求項 40】記録媒体に格納された情報を再生する情報再生処理をコンピュータ・システム上で実行せしめるコンピュータ・プログラムを提供するプログラム提供媒体であって、前記コンピュータ・プログラムは、  
記録媒体に格納されたコンテンツデータの読み取り態様と異なる特殊なデータ読み取り処理を実行し、記録媒体に格納された秘密情報を読み取る秘密情報復号処理ステップと、

20 前記秘密情報復号処理ステップにおいて記憶媒体から読み取られ復号された秘密情報をキー生成用データとしてコンテンツ復号キーを生成し、該コンテンツ復号キーに基づいて記録媒体から読み取られるデータの復号処理を実行する復号処理ステップと、  
を有することを特徴とするプログラム提供媒体。

【発明の詳細な説明】

【0001】

30 【発明の属する技術分野】本発明は、情報記録装置、情報再生装置、情報記録方法、情報再生方法、および情報記録媒体、並びにプログラム提供媒体に関し、特に、木構造の階層的鍵配信方式を用いることにより、メッセージ量を小さく抑さえ、マスターキーあるいはメディアキー等の鍵更新におけるデータ配信の負荷を軽減することを可能とした構成を提供するとともに、コンテンツの暗号処理用鍵の生成データとしてコンテンツの再生処理とは異なる特殊なデータ読み取り処理においてのみ読み取り可能な秘密情報を適用する構成により、コンテンツのセキュリティを高めることを可能とした情報記録装置、情報再生装置、情報記録方法、情報再生方法、および情報記録媒体、並びにプログラム提供媒体に関する。

40 【0002】具体的には、各記録再生器機器を n 分木の各葉 (リーフ) に配置した構成の鍵配信方法を用い、記録媒体もしくは通信回線を介して、コンテンツデータの記録媒体への記録もしくは記録媒体からの再生に必要な鍵 (マスターキーもしくはメディアキー) を配信し、これを用いて各装置がコンテンツデータの記録、再生を行うとともに、コンテンツ記録、再生用のコンテンツ格納ディスクにスタンパー ID 等を秘密情報として格納し、特定の再生処理によって秘密情報を取得して取得秘密情報に基づいてコンテンツの暗号処理用の鍵を生成する構成とした情報記録装置、情報再生装置、情報記録方法、  
50 情報再生方法、および情報記録媒体、並びにプログラム

提供媒体に関する。

【0003】

【従来の技術】デジタル信号処理技術の進歩、発展に伴い、近年においては、情報を、デジタル的に記録する記録装置や記録媒体が普及しつつある。このようなデジタル記録装置および記録媒体によれば、例えば画像や音声を劣化させることなく記録、再生を繰り返すことができる。このようにデジタルデータは画質や音質を維持したまま何度もコピーを繰り返し実行することができるため、コピーが違法に行われた記録媒体が市場に流通することになると、音楽、映画等各種コンテンツの著作権者、あるいは正当な販売権者等の利益が害されることになる。昨今では、このようなデジタルデータの不正なコピーを防ぐため、デジタル記録装置および記録媒体に違法なコピーを防止するための様々な仕組み（システム）が導入されている。

【0004】例えば、MD（ミニディスク）（MDは商標）装置において、違法なコピーを防止する方法として、SCMS（Serial Copy Management System）が採用されている。SCMSは、データ再生側において、オーディオデータとともにSCMS信号をデジタルインタフェース（DIF）から出力し、データ記録側において、再生側からのSCMS信号に基づいて、再生側からのオーディオデータの記録を制御することにより違法なコピーを防止するシステムである。

【0005】具体的にはSCMS信号は、オーディオデータが、何度でもコピーが許容されるコピーフリー（copy free）のデータであるか、1度だけコピーが許されている（copy once allowed）データであるか、またはコピーが禁止されている（copy prohibited）データであることを表す信号である。データ記録側において、DIFからオーディオデータを受信すると、そのオーディオデータとともに送信されるSCMS信号を検出する。そして、SCMS信号が、コピーフリー（copy free）となっている場合には、オーディオデータをSCMS信号とともにミニディスクに記録する。また、SCMS信号が、コピーを1度のみ許可（copy once allowed）となっている場合には、SCMS信号をコピー禁止（copy prohibited）に変更して、オーディオデータとともに、ミニディスクに記録する。さらに、SCMS信号が、コピー禁止（copy prohibited）となっている場合には、オーディオデータの記録を行わない。このようなSCMSを使用した制御を行なうことで、ミニディスク装置では、SCMSによって、著作権を有するオーディオデータが、違法にコピーされるのを防止するようになっている。

【0006】しかしながら、SCMSは上述のようにSCMS信号に基づいて再生側からのオーディオデータの記録を制御する構成をデータを記録する機器自体が有していることが前提であるため、SCMSの制御を実行す

る構成を持たないミニディスク装置が製造された場合には、対処するのが困難となる。そこで、例えば、DVDプレーヤでは、コンテンツ・スクランブルシステムを採用することにより、著作権を有するデータの違法コピーを防止する構成となっている。

【0007】コンテンツ・スクランブルシステムでは、DVD-ROM（Read Only Memory）に、ビデオデータやオーディオデータ等が暗号化されて記録されており、その暗号化されたデータを復号するのに用いるキー（復号鍵）が、ライセンスを受けたDVDプレーヤに与えられる。ライセンスは、不正コピーを行わない等の所定の動作規定に従うように設計されたDVDプレーヤに対して与えられる。従って、ライセンスを受けたDVDプレーヤでは、与えられたキーを利用して、DVD-ROMに記録された暗号化データを復号することにより、DVD-ROMから画像や音声を再生することができる。

【0008】一方、ライセンスを受けていないDVDプレーヤは、暗号化されたデータを復号するためのキーを有していないため、DVD-ROMに記録された暗号化データの復号を行うことができない。このように、コンテンツ・スクランブルシステム構成では、ライセンス時に要求される条件を満たしていないDVDプレーヤは、デジタルデータを記録したDVD-ROMの再生を行えないことになり、不正コピーが防止されるようになっている。

【0009】しかしながら、DVD-ROMで採用されているコンテンツ・スクランブルシステムは、ユーザによるデータの書き込みが不可能な記録媒体（以下、適宜、ROMメディアという）を対象としており、ユーザによるデータの書き込みが可能な記録媒体（以下、適宜、RAMメディアという）への適用については考慮されていない。

【0010】即ち、ROMメディアに記録されたデータが暗号化されていても、その暗号化されたデータを、そのまま全部、RAMメディアにコピーした場合には、ライセンスを受けた正当な装置で再生可能な、いわゆる海賊版を作成することができてしまう。

【0011】そこで、本出願人は、先の特許出願、特開平11-224461号公報（特願平10-25310号）において、個々の記録媒体を識別する為の情報（以下、媒体識別情報と記述する）を、他のデータとともに記録媒体に記録し、この媒体識別情報のライセンスを受けた装置であることを条件として、その条件が満たされた場合にのみ記録媒体の媒体識別情報へのアクセスが可能となる構成を提案した。

【0012】この方法では、記録媒体上のデータは、媒体識別情報とライセンスを受けることにより得られる秘密キー（マスターキー）により暗号化され、ライセンスを受けていない装置が、この暗号化されたデータを読み出したとしても、意味のあるデータを得ることができな

いようになっている。なお、装置はライセンスを受ける際、不正な複製（違法コピー）ができないように、その動作が規定される。

【0013】ライセンスを受けていない装置は、媒体識別情報にアクセスできず、また、媒体識別情報は個々の媒体毎に個別の値となっているため、ライセンスを受けていない装置が、記録媒体に記録されている、暗号化されたデータのすべてを新たな記録媒体に複製したとしても、そのようにして作成された記録媒体に記録されたデータは、ライセンスを受けていない装置は勿論、ライ

10  
【0014】

【発明が解決しようとする課題】ところで、上記の構成においては、ライセンスを受けた装置において格納されるマスターキーは全機器において共通であるのが一般的である。このように複数の機器に対して共通のマスターキーを格納するのは、1つの機器で記録された媒体を他の機器で再生可能とする（インターオペラビリティを確保する）ために必要な条件であるからである。

【0015】しかし、この方式においては、攻撃者が1つの機器の攻撃に成功し、マスターキーを取出した場合、全システムにおいて暗号化されて記録されているデータを復号することができてしまい、システム全体が崩壊する。これを防ぐためには、ある機器が攻撃されてマスターキーが露呈したことが発覚した場合、マスターキーを新たなものに更新し、攻撃に屈した機器以外の全機器に新たに更新されたマスターキーを与えることが必要になる。この構成を実現する一番単純な方式としては、個々の機器に固有の鍵（デバイスキー）を与えておき、新たなマスターキーを個々のデバイスキーで暗号化した値を用意し、記録媒体を介して機器に伝送する方式が考えられるが、機器の台数に比例して伝送すべき全メッセージ量が増加するという問題がある。

【0016】上記問題を解決する構成として、本出願人は、各情報記録再生装置をn分木の各葉（リーフ）に配置した構成の鍵配信方法を用い、記録媒体もしくは通信回線を介して、コンテンツデータの記録媒体への記録もしくは記録媒体からの再生に必要な鍵（マスターキーもしくはメディアキー）を配信し、これを用いて各装置がコンテンツデータの記録、再生を行うようにすることにより、正当な（秘密が露呈していない装置に）対して少ないメッセージ量でマスターキーもしくはメディアキーを伝送できる構成を、先に提案し、すでに特許出願している。具体的には、記録媒体への記録もしくは記録媒体からの再生に必要な鍵を生成するために必要となるキー、例えばn分木の各葉（リーフ）を構成するノードに割り当てたノードキーを更新ノードキーとして設定し、更新ノードキーを正当な機器のみが有するリーフキー、

ノードキーで復号可能な態様で暗号化処理した情報を含む有効化キープロック（EKB）を各情報記録再生装置に配信し、有効化キープロック（EKB）を受信した各情報記録再生装置のEKB復号処理により、各装置が記録もしくは記録媒体からの再生に必要な鍵を取得可能とした構成である。

【0017】上述の構成は、情報記録再生装置に与えられた暗号鍵や、記録媒体へのデータの記録／再生時の暗号化／復号処理に用いるメディアキーが露呈しないことにその安全性の根拠が置かれている。従って、メディアキーの露呈が防止可能であれば問題はない。しかし、秘密とされるべきメディアキーが露呈すると、少なからずシステムに影響があるものとなっている。

【0018】本発明は、上記の問題点を解決することを目的とするものであり、通常の方法で書き込んだ秘密情報を記録媒体へのデータの記録／再生時の暗号化／復号処理に用いる鍵生成用のデータとして用いる構成とすることにより、コンテンツの不正利用を排除可能とするとともに、記録／再生時の暗号化／復号処理に用いる鍵用の種データの漏洩の可能性を激減させたセキュリティの高い情報記録装置、情報再生装置、情報記録方法、情報再生方法、および情報記録媒体、並びにプログラム提供媒体を提供することを目的とする。

20  
【0019】

【課題を解決するための手段】本発明の第1の側面は、記録媒体に情報を記録する情報記録装置において、記録媒体に対する格納データの暗号化処理を実行する暗号処理手段と、記録媒体に格納されたコンテンツデータの読み取り態様と異なる特殊なデータ読み取り処理を実行し、記録媒体に格納された秘密情報を読み取る秘密情報復号処理手段と、を有し、前記暗号処理手段は、前記秘密情報復号処理手段において記憶媒体から読み取られ復号された秘密情報をキー生成用データとしてコンテンツ暗号化キーを生成し、該コンテンツ暗号化キーに基づいて記録媒体に格納するデータの暗号化処理を実行する構成を有することを特徴とする情報記録装置にある。

【0020】さらに、本発明の情報記録装置の一実施態様において、前記秘密情報は、記録媒体の製造時に記録媒体に格納され、複数の記録媒体において共通なスタンパーID、または個々の記録媒体に固有なディスクID、コンテンツ毎に異なって設定するコンテンツID、あるいは暗号処理用のキーのいずれかのデータを含み、前記秘密情報復号処理手段は、記録媒体から読み取られた秘密情報の復号処理を実行する構成を有することを特徴とする。

【0021】さらに、本発明の情報記録装置の一実施態様において、前記暗号処理手段は、前記秘密情報復号処理手段において読み取られた秘密情報を使用し、コンテンツ暗号化キーを生成する構成であり、読み取られた秘

密情報は情報記録装置外部からの読み取り可能な記憶手段への格納処理を行わず、前記暗号処理部内で実行されるコンテンツ暗号化キー生成処理においてのみ利用可能な構成としたことを特徴とする。

【0022】さらに、本発明の情報記録装置の一実施態様において、前記情報記録装置は、さらに、複数の異なる情報記録装置をリーフとした階層ツリー構造を構成する各ノードに固有のノードキーと各情報記録装置固有のリーフキーとを保有し、前記暗号処理手段は、前記秘密情報復号処理手段において読み取られた秘密情報と、前記情報記録装置に内蔵した暗号化キー生成用データに基づいて前記コンテンツ暗号化キーを生成する構成であり、前記暗号化キー生成用データは、ノードキーを下位階層のノードキーまたはリーフキーの少なくともいずれかを含むキーにより暗号化した有効化キープロック (EKB) によって更新可能なデータとして構成されていることを特徴とする。

【0023】さらに、本発明の情報記録装置の一実施態様において、前記暗号化キー生成用データは、複数の情報記録装置において共通なマスターキー、または特定の記録媒体に固有のメディアキーのいずれかであることを特徴とする。

【0024】さらに、本発明の情報記録装置の一実施態様において、前記暗号化キー生成用データは、更新情報としての世代番号が対応付けられた構成であり、前記暗号処理部は、前記記録媒体に対する暗号化データ格納時に、使用した前記暗号化キー生成用データの世代番号を記録時世代番号として前記記録媒体に格納する構成を有することを特徴とする。

【0025】さらに、本発明の情報記録装置の一実施態様において、トランスポートパケットから成るトランスポートストリームを構成する各パケットに受信時刻情報 (ATS) を付加するトランスポート・ストリーム処理手段を有し、前記暗号処理手段は、前記受信時刻情報 (ATS) の付加された1以上のパケットからなるブロックデータに対する暗号化キーとしてブロックキーを生成する構成を有し、前記記録媒体に対する格納データの暗号処理においては、前記秘密情報と、前記暗号化キー生成用データと前記受信時刻情報 (ATS) を含むブロックデータ固有の付加情報であるブロックシードとを含むデータに基づいて暗号化キーとしてのブロックキーを生成する構成を有することを特徴とする。

【0026】さらに、本発明の情報記録装置の一実施態様において、前記秘密情報復号処理手段は、秘密情報を形成するビット列を2進数系列により擾乱して記録媒体に格納されたデータの復号処理を実行する構成を有し、前記2進数系列を生成し、生成2進数系列と前記記録媒体からの再生信号との演算処理を実行して秘密情報の復号処理を実行する構成を有することを特徴とする。

【0027】さらに、本発明の情報記録装置の一実施態

様において、前記秘密情報復号処理手段は、秘密情報を構成する複数ビット単位に予め定められた規則に従って変換されて記録されたデータを記録媒体から読み取り、読み取りデータを再変換して秘密情報の復号処理を実行する構成を有することを特徴とする。

【0028】さらに、本発明の第2の側面は、記録媒体に記録された情報を再生する情報再生装置において、記録媒体から読み取られるデータの復号処理を実行する暗号処理手段と、記録媒体に格納されたコンテンツデータの読み取り態様と異なる特殊なデータ読み取り処理を実行し、記録媒体に格納された秘密情報を読み取る秘密情報復号処理手段と、を有し、前記暗号処理手段は、前記秘密情報復号処理手段において記憶媒体から読み取られ復号された秘密情報をキー生成用データとしてコンテンツ復号キーを生成し、該コンテンツ復号キーに基づいて記録媒体から読み取られるデータの復号処理を実行する構成を有することを特徴とする情報再生装置にある。

【0029】さらに、本発明の情報再生装置の一実施態様において、前記秘密情報は、記録媒体の製造時に記録媒体に格納され、複数の記録媒体において共通なスタンパーID、または個々の記録媒体に固有なディスクID、コンテンツ毎に異なって設定するコンテンツID、あるいは暗号処理用のキーのいずれかのデータを含み、前記秘密情報復号処理手段は、記録媒体から読み取られた秘密情報の復号処理を実行する構成を有することを特徴とする。

【0030】さらに、本発明の情報再生装置の一実施態様において、前記暗号処理手段は、前記秘密情報復号処理手段において読み取られた秘密情報を使用し、コンテンツ復号キーを生成する構成であり、読み取られた秘密情報は情報記録装置外部からの読み取り可能な記憶手段への格納処理を行わず、前記暗号処理部内で実行されるコンテンツ復号キー生成処理においてのみ利用可能な構成を有することを特徴とする。

【0031】さらに、本発明の情報再生装置の一実施態様において、複数の異なる情報再生装置をリーフとした階層ツリー構造を構成する各ノードに固有のノードキーと各情報再生装置固有のリーフキーとを保有し、前記暗号処理手段は、前記秘密情報復号処理手段において読み取られた秘密情報と、前記情報再生装置に内蔵した復号キー生成用データに基づいて前記コンテンツ復号キーを生成する構成であり、前記復号キー生成用データは、ノードキーを下位階層のノードキーまたはリーフキーの少なくともいずれかを含むキーにより暗号化した有効化キープロック (EKB) によって更新可能なデータとして構成されていることを特徴とする。

【0032】さらに、本発明の情報再生装置の一実施態様において、前記復号キー生成用データは、複数の情報再生装置において共通なマスターキー、または特定の記録媒体に固有のメディアキーのいずれかであることを特

徴とする。

【0033】さらに、本発明の情報再生装置の一実施態様において、前記復号キー生成用データは、更新情報としての世代番号が対応付けられた構成であり、前記暗号処理部は、前記記録媒体からのデータ再生時に、使用した前記復号キー生成用データの世代番号を記録時世代番号として前記記録媒体に格納する構成を有することを特徴とする。

【0034】さらに、本発明の情報再生装置の一実施態様において、トランスポートパケットから成るトランスポートストリームを構成する各パケットに受信時刻情報 (ATS) を付加するトランスポート・ストリーム処理手段を有し、前記暗号処理手段は、前記受信時刻情報 (ATS) の付加された1以上のパケットからなるブロックデータに対する暗号化キーとしてブロックキーを生成する構成を有し、前記記録媒体からのデータの復号処理においては、前記秘密情報と、前記復号キー生成用データと前記受信時刻情報 (ATS) を含むブロックデータ固有の付加情報であるブロックシードとを含むデータに基づいて復号キーとしてのブロックキーを生成する構成を有することを特徴とする。

【0035】さらに、本発明の情報再生装置の一実施態様において、前記秘密情報復号処理手段は、秘密情報を形成するビット列を2進数系列により擾乱して記録媒体に格納されたデータの復号処理を実行する構成を有し、前記2進数系列を生成し、生成2進数系列と前記記録媒体からの再生信号との演算処理を実行して秘密情報の復号処理を実行する構成を有することを特徴とする。

【0036】さらに、本発明の情報再生装置の一実施態様において、前記秘密情報復号処理手段は、秘密情報を構成する複数ビット単位に予め定められた規則に従って変換されて記録されたデータを記録媒体から読み取り、読み取りデータを再変換して秘密情報の復号処理を実行する構成を有することを特徴とする。

【0037】さらに、本発明の第3の側面は、記録媒体に情報を記録する情報記録方法において、記録媒体に格納されたコンテンツデータの読み取り態様と異なる特殊なデータ読み取り処理を実行し、記録媒体に格納された秘密情報を読み取る秘密情報復号処理ステップと、前記秘密情報復号処理ステップにおいて記憶媒体から読み取られ復号された秘密情報をキー生成用データとしてコンテンツ暗号化キーを生成し、該コンテンツ暗号化キーに基づいて記録媒体に格納するデータの暗号処理を実行する暗号処理ステップと、を有することを特徴とする情報記録方法にある。

【0038】さらに、本発明の情報記録方法の一実施態様において、前記秘密情報は、記録媒体の製造時に記録媒体に格納され、複数の記録媒体において共通なスタンパーID、または個々の記録媒体に固有なディスクID、コンテンツ毎に異なって設定するコンテンツID、

あるいは暗号処理用のキーのいずれかのデータを含み、前記秘密情報復号処理ステップは、記録媒体から読み取られた秘密情報の復号処理を実行することを特徴とする。

【0039】さらに、本発明の情報記録方法の一実施態様において、前記暗号処理ステップは、前記秘密情報復号処理手段において読み取られた秘密情報を使用し、コンテンツ暗号化キーを生成するステップを含み、読み取られた秘密情報は情報記録装置外部からの読み取り可能な記憶手段への格納処理を行わず、前記暗号処理部内で実行されるコンテンツ暗号化キー生成処理においてのみ利用可能としたことを特徴とする。

【0040】さらに、本発明の情報記録方法の一実施態様において、前記暗号処理ステップは、前記秘密情報復号処理手段において読み取られた秘密情報と、情報記録装置に内蔵した暗号化キー生成用データに基づいて前記コンテンツ暗号化キーを生成するステップを含み、前記暗号化キー生成用データは、複数の異なる情報記録装置をリーフとし、各分岐をノードとして各ノード、リーフに固有のキーを設定した階層ツリー構造のノードキーを下位階層のノードキーまたはリーフキーの少なくともいずれかを含むキーにより暗号化した有効化キーブロック (EKB) によって更新可能なデータであることを特徴とする。

【0041】さらに、本発明の情報記録方法の一実施態様において、前記暗号化キー生成用データは、複数の情報記録装置において共通なマスターキー、または特定の記録媒体に固有のメディアキーのいずれかであることを特徴とする。

【0042】さらに、本発明の情報記録方法の一実施態様において、前記暗号化キー生成用データは、更新情報としての世代番号が対応付けられた構成であり、前記暗号処理ステップは、前記記録媒体に対する暗号化データ格納時に、使用した前記暗号化キー生成用データの世代番号を記録時世代番号として前記記録媒体に格納するステップを含むことを特徴とする。

【0043】さらに、本発明の情報記録方法の一実施態様において、前記情報記録方法は、さらに、トランスポートパケットから成るトランスポートストリームを構成する各パケットに受信時刻情報 (ATS) を付加するトランスポート・ストリーム処理ステップを有し、前記暗号処理ステップは、前記受信時刻情報 (ATS) の付加された1以上のパケットからなるブロックデータに対する暗号化キーとしてブロックキーを生成するステップを含み、前記記録媒体に対する格納データの暗号処理においては、前記秘密情報と、前記暗号化キー生成用データと前記受信時刻情報 (ATS) を含むブロックデータ固有の付加情報であるブロックシードとを含むデータに基づいて暗号化キーとしてのブロックキーを生成することを特徴とする。

【0044】さらに、本発明の情報記録方法の一実施態様において、前記秘密情報復号処理ステップは、秘密情報を形成するビット列を2進数系列により擾乱して記録媒体に格納されたデータの復号処理を実行する復号処理ステップを含み、該復号処理ステップは、前記2進数系列を生成し、生成2進数系列と前記記録媒体からの再生信号との演算処理を実行して秘密情報の復号処理を実行することを特徴とする。

【0045】さらに、本発明の情報記録方法の一実施態様において、前記秘密情報復号処理ステップは、秘密情報を構成する複数ビット単位に予め定められた規則に従って変換されて記録されたデータを記録媒体から読み取り、読み取りデータを再変換して秘密情報の復号処理を実行することを特徴とする。

【0046】さらに、本発明の第4の側面は、記録媒体から情報を再生する情報再生方法において、記録媒体に格納されたコンテンツデータの読み取り態様と異なる特殊なデータ読み取り処理を実行し、記録媒体に格納された秘密情報を読み取る秘密情報復号処理ステップと、前記秘密情報復号処理ステップにおいて記憶媒体から読み取られ復号された秘密情報をキー生成用データとしてコンテンツ復号キーを生成し、該コンテンツ復号キーに基づいて記録媒体から読み取られるデータの復号処理を実行する復号処理ステップと、を有することを特徴とする情報再生方法にある。

【0047】さらに、本発明の情報再生方法の一実施態様において、前記秘密情報は、記録媒体の製造時に記録媒体に格納され、複数の記録媒体において共通なスタンパーID、または個々の記録媒体に固有なディスクID、コンテンツ毎に異なって設定するコンテンツID、あるいは暗号処理用のキーのいずれかのデータを含み、前記秘密情報復号処理ステップは、記録媒体から読み取られた秘密情報の復号処理を実行することを特徴とする。

【0048】さらに、本発明の情報再生方法の一実施態様において、前記復号処理ステップは、前記秘密情報復号処理手段において読み取られた秘密情報を使用し、コンテンツ復号キーを生成するステップを含み、読み取られた秘密情報は情報記録装置外部からの読み取り可能な記憶手段への格納処理を行わず、前記暗号処理部内で実行されるコンテンツ復号キー生成処理においてのみ利用可能としたことを特徴とする。

【0049】さらに、本発明の情報再生方法の一実施態様において、前記復号処理ステップは、前記秘密情報復号処理手段において読み取られた秘密情報と、情報再生装置に内蔵した復号キー生成用データに基づいて前記コンテンツ復号キーを生成するステップを含み、前記復号キー生成用データは、複数の異なる情報再生装置をリーフとし、各分岐をノードとして各ノード、リーフに固有のキーを設定した階層ツリー構造のノードキーを下位階

層のノードキーまたはリーフキーの少なくともいずれかを含むキーにより暗号化した有効化キープロック (EKB) によって更新可能なデータであることを特徴とする。

【0050】さらに、本発明の情報再生方法の一実施態様において、前記復号キー生成用データは、複数の情報再生装置において共通なマスターキー、または特定の記録媒体に固有のメディアキーのいずれかであることを特徴とする。

【0051】さらに、本発明の情報再生方法の一実施態様において、前記復号キー生成用データは、更新情報としての世代番号が対応付けられた構成であり、前記復号処理ステップは、前記記録媒体からのデータ再生時に、使用した前記復号キー生成用データの世代番号を記録時世代番号として前記記録媒体に格納するステップを含むことを特徴とする。

【0052】さらに、本発明の情報再生方法の一実施態様において、トランスポートパケットから成るトランスポートストリームを構成する各パケットに受信時刻情報 (ATS) を付加するトランスポート・ストリーム処理ステップを有し、前記復号処理ステップは、前記受信時刻情報 (ATS) の付加された1以上のパケットからなるブロックデータに対する暗号化キーとしてブロックキーを生成するステップを含み、前記記録媒体からのデータの再生処理においては、前記秘密情報と、前記復号キー生成用データと前記受信時刻情報 (ATS) を含むブロックデータ固有の付加情報であるブロックシードとを含むデータに基づいて復号キーとしてのブロックキーを生成することを特徴とする。

【0053】さらに、本発明の情報再生方法の一実施態様において、前記秘密情報復号処理ステップは、秘密情報を形成するビット列を2進数系列により擾乱して記録媒体に格納されたデータの復号処理を実行する復号処理ステップを含み、該復号処理ステップは、前記2進数系列を生成し、生成2進数系列と前記記録媒体からの再生信号との演算処理を実行して秘密情報の復号処理を実行することを特徴とする。

【0054】さらに、本発明の情報再生方法の一実施態様において、前記秘密情報復号処理ステップは、秘密情報を構成する複数ビット単位に予め定められた規則に従って変換されて記録されたデータを記録媒体から読み取り、読み取りデータを再変換して秘密情報の復号処理を実行することを特徴とする。

【0055】さらに、本発明の第5の側面は、情報を記録可能な情報記録媒体であって、通常格納データの読み取り態様と異なる特殊なデータ読み取り処理を実行することによってのみ再生可能な秘密情報と、該秘密情報を適用して生成可能な暗号処理鍵により復号可能な暗号化コンテンツを格納したことを特徴とする情報記録媒体にある。

【0056】さらに、本発明の情報記録媒体の一実施態様において、前記秘密情報は、複数の記録媒体において共通なスタンパーID、または個々の記録媒体に固有なディスクID、コンテンツ毎に異なって設定するコンテンツID、あるいは暗号処理用のキーのいずれかのデータを含むことを特徴とする。

【0057】さらに、本発明の第6の側面は、記録媒体に情報を記録する情報記録処理をコンピュータ・システム上で実行せしめるコンピュータ・プログラムを提供するプログラム提供媒体であって、前記コンピュータ・プログラムは、記録媒体に格納されたコンテンツデータの読み取り態様と異なる特殊なデータ読み取り処理を実行し、記録媒体に格納された秘密情報を読み取る秘密情報復号処理ステップと、前記秘密情報復号処理ステップにおいて記憶媒体から読み取られ復号された秘密情報をキー生成用データとしてコンテンツ暗号化キーを生成し、該コンテンツ暗号化キーに基づいて記録媒体に格納するデータの暗号処理を実行する暗号処理ステップと、を有することを特徴とするプログラム提供媒体にある。

【0058】さらに、本発明の第7の側面は、記録媒体に格納された情報を再生する情報再生処理をコンピュータ・システム上で実行せしめるコンピュータ・プログラムを提供するプログラム提供媒体であって、前記コンピュータ・プログラムは、記録媒体に格納されたコンテンツデータの読み取り態様と異なる特殊なデータ読み取り処理を実行し、記録媒体に格納された秘密情報を読み取る秘密情報復号処理ステップと、前記秘密情報復号処理ステップにおいて記憶媒体から読み取られ復号された秘密情報をキー生成用データとしてコンテンツ復号キーを生成し、該コンテンツ復号キーに基づいて記録媒体から読み取られるデータの復号処理を実行する復号処理ステップと、を有することを特徴とするプログラム提供媒体にある。

【0059】

【作用】本発明の構成においては、記録媒体に、あらかじめその書き込み／読出し方法の解析の困難な秘密情報からなる信号を埋め込んでおく。この記録媒体に対してデータの記録／再生を行う際のデータの暗号化／復号処理を行うための暗号鍵には、上記の秘密情報を作用させる。秘密情報の読出し方法および読み出された秘密の値は記録再生装置内でたとえばLSI内に実装されて高度に保護され、露呈しない構成である。このような構成であるため、たとえ他の暗号鍵が露呈したとしても、記録媒体上に秘密情報として格納されたデータは安全に保護できる。また、記録媒体上の音楽等の各種コンテンツデータの暗号化／復号処理を行うための暗号鍵は、秘密情報を用いて生成されることになるため、コンテンツ自体の不正な復号等の処理が困難になり、セキュリティレベルの高いコンテンツ保護が可能になる。

【0060】なお、本発明の第6および第7の側面に係

るプログラム提供媒体は、例えば、様々なプログラム・コードを実行可能な汎用コンピュータ・システムに対して、コンピュータ・プログラムをコンピュータ可読な形式で提供する媒体である。媒体は、CDやFD、MOなどの記録媒体、あるいは、ネットワークなどの伝送媒体など、その形態は特に限定されない。

【0061】このようなプログラム提供媒体は、コンピュータ・システム上で所定のコンピュータ・プログラムの機能を実現するための、コンピュータ・プログラムと提供媒体との構造上又は機能上の協働的關係を定義したものである。換言すれば、該提供媒体を介してコンピュータ・プログラムをコンピュータ・システムにインストールすることによって、コンピュータ・システム上では協働的作用が発揮され、本発明の他の側面と同様の作用効果を得ることができるのである。

【0062】本発明のさらに他の目的、特徴や利点は、後述する本発明の実施例や添付する図面に基づくより詳細な説明によって明らかになるであろう。

【0063】

【発明の実施の形態】〔システム構成〕図1は、本発明を適用した記録再生装置100の一実施例構成を示すブロック図である。記録再生装置100は、入出力I/F (Interface) 120、MPEG (Moving Picture Experts Group) コーデック130、A/D、D/Aコンバータ141を備えた入出力I/F (Interface) 140、暗号処理手段150、ROM (Read Only Memory) 160、CPU (Central Processing Unit) 170、メモリ180、記録媒体195のドライブ190、さらにトランスポート・ストリーム処理手段 (TS処理手段) 300、秘密情報復号処理手段50を有し、これらはバス110によって相互に接続されている。

【0064】入出力I/F 120は、外部から供給される画像、音声、プログラム等の各種コンテンツを構成するデジタル信号を受信し、バス110上に出力するとともに、バス110上のデジタル信号を受信し、外部に出力する。MPEGコーデック130は、バス110を介して供給されるMPEG符号化されたデータを、MPEGデコードし、入出力I/F 140に出力するとともに、入出力I/F 140から供給されるデジタル信号をMPEGエンコードしてバス110上に出力する。入出力I/F 140は、A/D、D/Aコンバータ141を内蔵している。入出力I/F 140は、外部から供給されるコンテンツとしてのアナログ信号を受信し、A/D、D/Aコンバータ141でA/D (Analog Digital) 変換することで、デジタル信号として、MPEGコーデック130に出力するとともに、MPEGコーデック130からのデジタル信号を、A/D、D/Aコンバータ141でD/A (Digital Analog) 変換することで、アナログ信号として、外部に出力する。

【0065】暗号処理手段150は、例えば、1チップ

のLSI (Large Scale IntegratedCircuit)で構成され、バス110を介して供給されるコンテンツとしてのデジタル信号を暗号化し、または復号し、バス110上に出力する構成を持つ。なお、暗号処理手段150は1チップLSIに限らず、各種のソフトウェアまたはハードウェアを組み合わせた構成によって実現することも可能である。ソフトウェア構成による処理手段としての構成については後段で説明する。

【0066】ROM160は、例えば、記録再生装置ごとに固有の、あるいは複数の記録再生装置のグループごとに固有のデバイスキーであるリーフキーと、複数の記録再生装置、あるいは複数のグループに共有のデバイスキーであるノードキーを記憶している。CPU170は、メモリ180に記憶されたプログラムを実行することで、MPEGコーデック130や暗号処理手段150等を制御する。メモリ180は、例えば、不揮発性メモリで、CPU170が実行するプログラムや、CPU170の動作上必要なデータを記憶する。ドライブ190は、デジタルデータを記録再生可能な記録媒体195を駆動することにより、記録媒体195からデジタルデータを読み出し（再生し）、バス110上に出力するとともに、バス110を介して供給されるデジタルデータを、記録媒体195に供給して記録させる。また、プログラムをROM160に、デバイスキーをメモリ180に記憶するようにしてもよい。

【0067】記録媒体195は、例えば、DVD、CD等の光ディスク、光磁気ディスク、磁気ディスク、磁気テープ、あるいはRAM等の半導体メモリ等のデジタルデータの記憶可能な媒体であり、本実施の形態では、ドライブ190に対して着脱可能な構成であるとする。但し、記録媒体195は、記録再生装置100に内蔵する構成としてもよい。

【0068】トランスポート・ストリーム処理手段（TS処理手段）300は、後段において図6以下を用いて詳細に説明するが、例えば複数のTVプログラム（コンテンツ）が多重化されたトランスポートストリームから特定のプログラム（コンテンツ）に対応するトランスポートパケットを取り出して、取り出したトランスポートストリームの出現タイミング情報を各パケットとともに記録媒体195に格納するためのデータ処理および、記録媒体195からの再生処理時の出現タイミング制御処理を行なう。

【0069】トランスポートストリームには、各トランスポートパケットの出現タイミング情報としてのATS（Arrival Time Stamp：着信時刻スタンプ）が設定されており、このタイミングはMPEG2システムズで規定されている仮想的なデコーダであるT-STD (Transport stream System Target Decoder)を破綻させないように符号化時に決定され、トランスポートストリームの再生時には、各トランスポートパケットに付加された

ATSによって出現タイミングを制御する。トランスポート・ストリーム処理手段（TS処理手段）300は、これらの制御を実行する。例えば、トランスポートパケットを記録媒体に記録する場合には、各パケットの間隔を詰めたソースパケットとして記録するが、各トランスポートパケットの出現タイミングを併せて記録媒体に保存することにより、再生時に各パケットの出力タイミングを制御することが可能となる。トランスポート・ストリーム処理手段（TS処理手段）300は、DVD等の記録媒体195へのデータ記録時に、各トランスポートパケットの入力タイミングを表すATS（Arrival Time Stamp：着信時刻スタンプ）を付加して記録する。

【0070】本発明の記録再生装置100は、上述のATSの付加されたトランスポートストリームによって構成されるコンテンツについて、暗号処理手段150において暗号化処理を実行し、暗号化処理のなされたコンテンツを記録媒体195に格納する。さらに、暗号処理手段150は、記録媒体195に格納された暗号化コンテンツの復号処理を実行する。これらの処理の詳細については、後段で説明する。

【0071】秘密情報復号処理手段500は、記録媒体195に格納された特殊な再生処理により読み取り可能な秘密情報の再生、復号処理を実行する処理手段である。記録媒体195に格納される秘密情報は、例えばディスクの製造磁のスタンパー毎に設定されるスタンパーID、ディスク毎に異なって設定されるディスクID、コンテンツ毎に異なって設定するコンテンツID、あるいは暗号処理用のキー等、様々な識別データ、暗号処理鍵等である。

【0072】秘密情報復号処理手段500は、記録媒体195に格納された秘密情報を読み取り復号し、復号した秘密情報を暗号処理手段150に転送する。暗号処理手段150は、秘密情報を用いて記録媒体に対するコンテンツ記録、再生時に適用する暗号処理鍵を生成する。秘密情報復号処理手段500において復号された秘密情報は記録再生装置外部からの読み取り可能な記憶手段への格納処理を行わず、暗号処理手段150内で実行されるコンテンツ暗号化キー生成においてのみ使用される構成であり、秘密情報の外部への漏洩を防止した構成となっている。

【0073】なお、図1に示す暗号処理手段150、TS処理手段300、秘密情報復号処理手段500は、理解を容易にするため、別ブロックとして示してあるが、各機能を実行する1つまたは複数のLSIとして構成してもよく、また、各機能のいずれかをソフトウェアまたはハードウェアを組み合わせた構成によって実現する構成としてもよい。

【0074】本発明の記録再生装置の構成例としては図1に示す構成の他に図2に示す構成が可能である。図2に示す記録再生装置200では、記録媒体205はドラ

イブ装置としての記録媒体インタフェース (I/F) 210 から着脱が可能であり、この記録媒体 205 を別の記録再生装置に装着してもデータの読出し、書きこみが可能な構成としたものである。

【0075】 [データ記録処理およびデータ再生処理] 次に、図1あるいは図2の記録再生装置における記録媒体に対するデータ記録処理および記録媒体からのデータ再生処理について、図3および図4のフローチャートを参照して説明する。外部からのデジタル信号のコンテンツを、記録媒体 195 に記録する場合においては、図3 (A) のフローチャートにしたがった記録処理が行われる。即ち、デジタル信号のコンテンツ (デジタルコンテンツ) が、例えば、IEEE (Institute of Electrical and Electronics Engineers) 1394 シリアルバス等を介して、入出力 I/F 120 に供給されると、ステップ S301 において、入出力 I/F 120 は、供給されるデジタルコンテンツを受信し、バス 110 を介して、TS 処理手段 300 に出力する。

【0076】 TS 処理手段 300 は、ステップ S302 において、トランスポートストリームを構成する各トランスポートパケットに A TS を付加したブロックデータを生成して、バス 110 を介して、暗号処理手段 150 に出力する。

【0077】 暗号処理手段 150 は、ステップ S303 において、受信したデジタルコンテンツに対する暗号化処理を実行し、その結果得られる暗号化コンテンツを、バス 110 を介して、ドライブ 190、あるいは記録媒体 I/F 210 に出力する。暗号化コンテンツは、ドライブ 190、あるいは記録媒体 I/F 210 を介して記録媒体 195 に記録 (S304) され、記録処理を終了する。なお、暗号処理手段 150 における暗号処理については後段で説明する。

【0078】 なお、IEEE1394 シリアルバスを介して接続した装置相互間で、デジタルコンテンツを伝送するときの、デジタルコンテンツを保護するための規格として、本特許出願人であるソニー株式会社を含む 5 社によって、5CDTCP (Five Company Digital Transmission Content Protection) (以下、適宜、DTCP という) が定められているが、この DTCP では、コピーフリーでないデジタルコンテンツを装置相互間で伝送する場合、データ伝送に先立って、送信側と受信側が、コピーを制御するためのコピー制御情報を正しく取り扱えるかどうかの認証を相互に行い、その後、送信側において、デジタルコンテンツを暗号化して伝送し、受信側において、その暗号化されたデジタルコンテンツ (暗号化コンテンツ) を復号するようになっている。

【0079】 この DTCP に規格に基づくデータ送受信においては、データ受信側の入出力 I/F 120 は、ステップ S301 で、IEEE1394 シリアルバスを介して暗号化コンテンツを受信し、その暗号化コンテンツを、DT

CP に規格に準拠して復号し、平文のコンテンツとして、その後、暗号処理手段 150 に出力する。

【0080】 DTCP によるデジタルコンテンツの暗号化は、時間変化するキーを生成し、そのキーを用いて行われる。暗号化されたデジタルコンテンツは、その暗号化に用いたキーを含めて、IEEE1394 シリアルバス上を伝送され、受信側では、暗号化されたデジタルコンテンツを、そこに含まれるキーを用いて復号する。

【0081】 なお、DTCP によれば、正確には、キーの初期値と、デジタルコンテンツの暗号化に用いるキーの変更タイミングを表すフラグとが、暗号化コンテンツに含まれる。そして、受信側では、その暗号化コンテンツに含まれるキーの初期値を、やはり、その暗号化コンテンツに含まれるフラグのタイミングで変更していくことで、暗号化に用いられたキーが生成され、暗号化コンテンツが復号される。但し、ここでは、暗号化コンテンツに、その復号を行うためのキーが含まれていると等価であると考えても差し支えないため、以下では、そのように考えるものとする。ここで、DTCP については、例えば、<http://www.dtcp.com> の URL (Uniform Resource Locator) で特定される Web ページにおいて、インフォメショナルバージョン (Informational Version) の取得が可能である。

【0082】 次に、外部からのアナログ信号のコンテンツを、記録媒体 195 に記録する場合の処理について、図3 (B) のフローチャートに従って説明する。アナログ信号のコンテンツ (アナログコンテンツ) が、入出力 I/F 140 に供給されると、入出力 I/F 140 は、ステップ S321 において、そのアナログコンテンツを受信し、ステップ S322 に進み、内蔵する A/D、D/A コンバータ 141 で A/D 変換して、デジタル信号のコンテンツ (デジタルコンテンツ) とする。

【0083】 このデジタルコンテンツは、MPEG コーデック 130 に供給され、ステップ S323 において、MPEG エンコード、すなわち MPEG 圧縮による符号化処理が実行され、バス 110 を介して、暗号処理手段 150 に供給される。

【0084】 以下、ステップ S324、S325、S326 において、図3 (A) のステップ S302、S303 における処理と同様の処理が行われる。すなわち、TS 処理手段 300 によるトランスポートパケットに対する A TS 付加、暗号処理手段 150 における暗号化処理が実行され、その結果得られる暗号化コンテンツを、記録媒体 195 に記録して、記録処理を終了する。

【0085】 次に、記録媒体 195 に記録されたコンテンツを再生して、デジタルコンテンツ、あるいはアナログコンテンツとして出力する処理について図4のフローに従って説明する。デジタルコンテンツとして外部に出力する処理は図4 (A) のフローチャートにしたがった再生処理として実行される。即ち、まず最初に、ス

ステップS401において、ドライブ190または記録媒体1/F210によって、記録媒体195に記録された暗号化コンテンツが読み出され、バス110を介して、暗号処理手段150に出力される。

【0086】暗号処理手段150では、ステップS402において、ドライブ190または記録媒体1/F210から供給される暗号化コンテンツが復号処理され、復号データがバス110を介して、TS処理手段300に出力される。

【0087】TS処理手段300は、ステップS403 10において、トランスポートストリームを構成する各トランスポートパケットのATSから出力タイミングを判定し、ATSに応じた制御を実行して、バス110を介して、入出力I/F120に供給する。入出力I/F120は、TS処理手段300からのデジタルコンテンツを、外部に出力し、再生処理を終了する。なお、TS処理手段300の処理、暗号処理手段150におけるデジタルコンテンツの復号処理については後述する。

【0088】なお、入出力I/F120は、ステップS404で、IEEE1394シリアルバスを介してデジタルコ 20ンテンツを出力する場合には、DTC Pの規格に準拠して、上述したように、相手の装置との間で認証を相互に行い、その後、デジタルコンテンツを暗号化して伝送する。

【0089】記録媒体195に記録されたコンテンツを再生して、アナログコンテンツとして外部に出力する場合においては、図4(B)のフローチャートに従った再生処理が行われる。

【0090】即ち、ステップS421、S422、S423において、図4(A)のステップS401、S40 302、S403における場合とそれぞれ同様の処理が行われ、これにより、暗号処理手段150において得られた復号されたデジタルコンテンツは、バス110を介して、MPEGコーデック130に供給される。

【0091】MPEGコーデック130では、ステップS424において、デジタルコンテンツがMPEGデコード、すなわち伸長処理が実行され、入出力I/F140に供給される。入出力I/F140は、ステップS424において、MPEGコーデック130でMPEGデコードされたデジタルコンテンツを、内蔵するA/D、D/Aコンバータ141でD/A変換(S425)して、アナログコンテンツとする。そして、ステップS426に進み、入出力I/F140は、そのアナログコ 40ンテンツを、外部に出力し、再生処理を終了する。

【0092】〔データフォーマット〕次に、図5を用いて、本発明における記録媒体上のデータフォーマットを説明する。本発明における記録媒体上のデータの読み書きの最小単位をブロック(block)という名前と呼ぶ。1ブロックは、 $192 \times X$  (エックス) バイト (例えば  $X = 32$ ) の大きさとなっている。

【0093】本発明では、MPEG2のTS (トランスポート・ストリーム) パケット (188バイト) にATSを付加して192バイトとして、それをX個集めて1ブロックのデータとしている。ATSは24乃至32ビットの着信時刻を示すデータであり、先にも説明したようにArrival Time Stamp (着信時刻スタンプ) の略である。ATSは各パケットの着信時刻に応じたランダム性のあるデータとして構成される。記録媒体のひとつのブロック (セクタ) には、ATSを付加したTS (トランスポート・ストリーム) パケットをX個記録する。本発明の構成では、トランスポートストリームを構成する各ブロックの第1番目のTSパケットに付加されたATSを用いてそのブロック (セクタ) のデータを暗号化するブロックキーを生成する。

【0094】ランダム性のあるATSを用いて暗号化用のブロックキーを生成することにより、ブロック毎に異なる固有キーが生成される。生成されたブロック固有キーを用いてブロック毎の暗号化処理を実行する。また、ATSを用いてブロックキーを生成する構成とすることにより、各ブロック毎の暗号化鍵を格納するための記録媒体上の領域が不要となり、メインデータ領域が有効に使用可能となる。さらに、データの記録、再生時にメインデータ部以外のデータをアクセスする必要もなくなり、処理が効率的になる。

【0095】なお、図5に示すブロック・シード (Block Seed) は、ATSを含む付加情報である。ブロック・シードは、さらにATSだけでなくコピー制御情報 (CCI: Copy Control Information) も付加した構成としてもよい。この場合、ATSとCCIを用いてブロックキーを生成する構成とすることができる。

【0096】なお、ここで、ブロック・シードに含まれるコピー制限情報 (CCI: Copy Control Information) は、後段で説明するが、企業5社の共同提案としての5CDTCP (Digital Transmission Content Protection) システムで提唱するコピー制御情報 (CCI: Copy Control Information) であり、デバイスの能力に応じた2種類の情報、すなわち、EMI (Encryption Mode Indicator)、あるいは、コピー制御情報を送るための場所があらかじめ確保されているようなフォーマットにおいて適用されるコンテンツに埋め込まれたコピー制御情報 (CCI) である埋め込みCCI (Embedded CCI) のいずれかの情報を反映したものとなる。

【0097】なお、本発明の構成においては、DVD等の記録媒体上にデータを格納する場合、コンテンツの大部分のデータは暗号化されるが、図5の最下段に示すように、ブロックの先頭のm (たとえば、 $m = 8$  または  $16$ ) バイトは暗号化されずに平文 (Unencrypted data) のまま記録され、残りのデータ ( $m + 1$  バイト以降) が暗号化される。これは暗号処理が8バイト単位としての 50 処理であるために暗号処理データ長 (Encrypted data)

に制約が発生するためである。なお、もし、暗号処理が 8 バイト単位でなく、たとえば 1 バイト単位で行なえるなら、 $m=4$  として、ブロックシード以外の部分をすべて暗号化してもよい。

【0098】[TS 処理手段における処理] ここで、ATS の機能について詳細に説明する。ATS は、先にも説明したように入力トランスポートストリーム中の各トランスポートパケットの出現タイミングを保存するために付加する着信時刻スタンプである。

【0099】すなわち、例えば複数の TV プログラム (コンテンツ) が多重化されたトランスポートストリームの中から 1 つまたは幾つかの TV プログラム (コンテンツ) を取り出した時、その取り出したトランスポートストリームを構成するトランスポートパケットは、不規則な間隔で現れる (図 7 (a) 参照)。トランスポートストリームは、各トランスポートパケットの出現タイミングに重要な意味があり、このタイミングは MPEG 2 システムズ (ISO/IEC 13818-1) で規定されている仮想的なデコーダである T-ST D (Transport stream System Target Decoder) を破綻させないように符号化時に決定される。

【0100】トランスポートストリームの再生時には、各トランスポートパケットに付加された ATS によって出現タイミングが制御される。従って、記録媒体にトランスポートパケットを記録する場合には、トランスポートパケットの入力タイミングを保存する必要がある、トランスポートパケットを DVD 等の記録媒体に記録する時に、各トランスポートパケットの入力タイミングを表す ATS を付加して記録する。

【0101】図 6 に、デジタルインタフェース経由で入力されるトランスポートストリームを DVD 等の記録媒体であるストレージメディアに記録する時の TS 処理手段 300 において実行する処理を説明するブロック図を示す。端子 600 からは、デジタル放送等のデジタルデータとしてトランスポートストリームが入力される。図 1 または図 2 においては、入出力 I/F 120 を介して、あるいは入出力 I/F 140、MPEG コーデック 130 を介して端子 600 からトランスポートストリームが入力される。

【0102】トランスポートストリームは、ビットストリームパーサ (parser) 602 に入力される。ビットストリームパーサ 602 は、入力トランスポートストリームの中から PCR (Program Clock Reference) パケットを検出する。ここで、PCR パケットとは、MPEG 2 システムズで規定されている PCR が符号化されているパケットである。PCR パケットは、100 msec 以内の時間間隔で符号化されている。PCR は、トランスポートパケットが受信側に到着する時刻を 27 MHz の精度で表す。

【0103】そして、27 MHz PLL 603 におい

て、記録再生器が持つ 27 MHz クロックをトランスポートストリームの PCR にロック (Lock) させる。タイムスタンプ発生回路 604 は、27 MHz クロックのクロックのカウント値に基づいたタイムスタンプを発生する。そして、ブロック・シード (Block seed) 付加回路 605 は、トランスポートパケットの第 1 バイト目がスミージングバッファ 606 へ入力される時のタイムスタンプを ATS として、そのトランスポートパケットに付加する。

【0104】ATS が付加されたトランスポートパケットは、スミージングバッファ 606 を通って、端子 607 から、暗号処理手段 150 に出力され、後段で説明する暗号処理が実行された後、ドライブ 190 (図 1)、記録媒体 I/F 210 (図 2) を介してストレージメディアである記録媒体 195 に記録される。

【0105】図 7 は、入力トランスポートストリームが記録媒体に記録される時の処理の例を示す。図 7 (a) は、ある特定プログラム (コンテンツ) を構成するトランスポートパケットの入力を示す。ここで横軸は、ストリーム上の時刻を示す時間軸である。この例ではトランスポートパケットの入力は、図 7 (a) に示すように不規則なタイミングで現れる。

【0106】図 7 (b) は、ブロック・シード (Block Seed) 付加回路 605 の出力を示す。ブロック・シード (Block Seed) 付加回路 605 は、トランスポートパケット毎に、そのパケットのストリーム上の時刻を示す ATS を含むブロック・シード (Block Seed) を付加して、ソースパケットを出力する。図 7 (c) は記録媒体に記録されたソースパケットを示す。ソースパケットは、図 7 (c) に示すように間隔を詰めて記録媒体に記録される。このように間隔を詰めて記録することにより記録媒体の記録領域を有効に使用できる。

【0107】図 8 は、記録媒体 195 に記録されたトランスポートストリームを再生する場合の TS 処理手段 300 の処理構成ブロック図を示している。端子 800 からは、後段で説明する暗号処理手段において復号された ATS 付きのトランスポートパケットが、ブロック・シード (Block seed) 分離回路 801 へ入力され、ATS とトランスポートパケットが分離される。タイミング発生回路 804 は、再生器が持つ 27 MHz クロック 805 のクロックカウンタ値に基づいた時間を計算する。

【0108】なお、再生の開始時において、一番最初の ATS が初期値として、タイミング発生回路 804 にセットされる。比較器 803 は、ATS とタイミング発生回路 804 から入力される現在の時刻を比較する。そして、タイミング発生回路 804 が発生する時間と ATS が等しくなった時、出力制御回路 802 は、そのトランスポートパケットを MPEG コーデック 130 またはデジタル入出力 I/F 120 へ出力する。

【0109】図 9 は、入力 AV 信号を記録再生器 100

のMPEGコーデック130においてMPEGエンコードして、さらにTS処理手段300においてトランスポートストリームを符号化する構成を示す。従って図9は、図1または、図2におけるMPEGコーデック130とTS処理手段300の両処理構成を併せて示すブロック図である。端子901からは、ビデオ信号が入力されており、それはMPEGビデオエンコーダ902へ入力される。

【0110】MPEGビデオエンコーダ902は、入力ビデオ信号をMPEGビデオストリームに符号化し、それをバッファビデオストリームバッファ903へ出力する。また、MPEGビデオエンコーダ902は、MPEGビデオストリームについてのアクセスユニット情報を多重化スケジューラ908へ出力する。ビデオストリームのアクセスユニットとは、ピクチャであり、アクセスユニット情報とは、各ピクチャのピクチャタイプ、符号化ビット量、デコードタイムスタンプである。ここで、ピクチャタイプは、I/P/Bピクチャ (picture) の情報である。また、デコードタイムスタンプは、MPEG 2システムズで規定されている情報である。

【0111】端子904からは、オーディオ信号が入力されており、それはMPEGオーディオエンコーダ905へ入力される。MPEGオーディオエンコーダ905は、入力オーディオ信号をMPEGオーディオストリームに符号化し、それをバッファ906へ出力する。また、MPEGオーディオエンコーダ905は、MPEGオーディオストリームについてのアクセスユニット情報を多重化スケジューラ908へ出力する。オーディオストリームのアクセスユニットとは、オーディオフレームであり、アクセスユニット情報とは、各オーディオフレームの符号化ビット量、デコードタイムスタンプである。

【0112】多重化スケジューラ908には、ビデオとオーディオのアクセスユニット情報が入力される。多重化スケジューラ908は、アクセスユニット情報に基づいて、ビデオストリームとオーディオストリームをトランスポートパケットに符号化する方法を制御する。多重化スケジューラ908は、内部に27MHz精度の基準時刻を発生するクロックを持ち、そして、MPEG 2で規定されている仮想的なデコーダモデルであるT-S-TDを満たすようにして、トランスポートパケットのパケット符号化制御情報を決定する。パケット符号化制御情報は、パケット化するストリームの種類とストリームの長さである。

【0113】パケット符号化制御情報がビデオパケットの場合、スイッチ976はa側になり、ビデオストリームバッファ903からパケット符号化制御情報により指示されたペイロードデータ長のビデオデータが読み出され、トランスポートパケット符号化器909へ入力される。

【0114】パケット符号化制御情報がオーディオパケットの場合、スイッチ976はb側になり、オーディオストリームバッファ906から指示されたペイロードデータ長のオーディオデータが読み出され、トランスポートパケット符号化器909へ入力される。

【0115】パケット符号化制御情報がPCRパケットの場合、トランスポートパケット符号化器909は、多重化スケジューラ908から入力されるPCRを取り込み、PCRパケットを出力する。パケット符号化制御情報がパケットを符号化しないことを指示する場合、トランスポートパケット符号化器909へは何も入力されない。

【0116】トランスポートパケット符号化器909は、パケット符号化制御情報がパケットを符号化しないことを指示する場合、トランスポートパケットを出力しない。それ以外の場合、パケット符号化制御情報に基づいてトランスポートパケットを生成し、出力する。したがって、トランスポートパケット符号化器909は、間欠的にトランスポートパケットを出力する。到着 (Arrival) タイムスタンプ (time stamp) 計算手段910は、多重化スケジューラ908から入力されるPCRに基づいて、トランスポートパケットの第1バイト目が受信側に到着する時刻を示すATSを計算する。

【0117】多重化スケジューラ908から入力されるPCRは、MPEG 2で規定されるトランスポートパケットの10バイト目の受信側への到着時刻を示すので、ATSの値は、PCRの時刻から10バイト前のバイトが到着する時刻となる。

【0118】ブロック・シード (Block Seed) 付加回路911は、トランスポートパケット符号化器909から出力されるトランスポートパケットにATSを付加する。ブロック・シード (Block seed) 付加回路911から出力されるATS付きのトランスポートパケットは、スムージングバッファ912を通して、暗号処理手段150へ入力され、後段で説明する暗号処理が実行された後、ストレージメディアである記録媒体195へ格納される。

【0119】記録媒体195へ格納されるATS付きのトランスポートパケットは、暗号処理手段150で暗号化される前に図7(c)に示すように間隔を詰めた状態で入力され、その後、記録媒体195に格納される。トランスポートパケットが間隔を詰めて記録されても、ATSを参照することによって、そのトランスポートパケットの受信側への入力時刻を制御することができる。

【0120】ところで、ATSの大きさは32ビットに決まっているわけではなく、24ビット乃至31ビットでも構わない。ATSのビット長が長いほど、ATSの時間カウンターが一周する周期が長くなる。例えば、ATSが27MHz精度のバイナリカウンターである場合、24-bit長のATSが一周する時間は、約0.6

秒である。この時間間隔は、一般のトランスポートストリームでは十分な大きさである。なぜなら、トランスポートストリームのパケット間隔は、MPEG2の規定により、最大0.1秒と決められているからである。しかしながら、十分な余裕を見て、ATSを24-bit以上にしても良い。

【0121】このように、ATSのビット長を様々な長さとした場合、ブロックデータの付加データであるブロックシードの構成としていくつかの構成が可能となる。ブロック・シードの構成例を図10に示す。図10の例1は、ATSを32ビット分使用する例である。図10の例2は、ATSを30ビットとし、コピー制御情報(CCI)を2ビット分使用する例である。コピー制御情報は、それが付加されたデータのコピー制御の状態を表す情報であり、SCMS: Serial Copy Management SystemやCGMS: Copy Generation Management Systemが有名である。これらのコピー制御情報では、その情報が付加されたデータは制限なくコピーが許可されていることを示すコピーフリー(Copy Free)、1世代のみのコピーを許可する1世代コピー許可(One Generation Copy Allowed)、コピーを認めないコピー禁止(Copy Prohibited)などの情報が表せる。

【0122】図10に示す例3は、ATSを24ビットとし、CCIを2ビット使用し、さらに他の情報を6ビット使用する例である。他の情報としては、たとえばこのデータがアナログ出力される際に、アナログ映像データのコピー制御機構であるマクロビジョン(Macrovision)のオン/オフ(On/Off)を示す情報など、様々な情報を利用することが可能である。

【0123】[キー配布構成としてのツリー(木)構造について]次に、図1または図2に示した記録再生装置が、データを記録媒体に記録、もしくは記録媒体から再生する際に必要なマスターキーを、各機器に配布する構成について説明する。図11は、本方式を用いた記録システムにおける記録再生装置の鍵の配布構成を示した図である。図11の最下段に示すナンバ0~15が個々の記録再生装置である。すなわち図11に示す木(ツリー)構造の各葉(リーフ: leaf)がそれぞれの記録再生装置に相当する。

【0124】各デバイス0~15は、製造時(出荷時)に、あらかじめ定められている初期ツリーにおける、自分のリーフからルートに至るまでのノードに割り当てられた鍵(ノードキー)および各リーフのリーフキーを自身で格納する。図11の最下段に示すK0000~K1111が各デバイス0~15にそれぞれ割り当てられたリーフキーであり、最上段のKRから、最下段から2番目の節(ノード)に記載されたキー: KR~K111をノードキーとする。

【0125】図11に示すツリー構成において、例えばデバイス0はリーフキーK0000と、ノードキー: K

000、K00、K0、KRを所有する。デバイス5はK0101、K010、K01、K0、KRを所有する。デバイス15は、K1111、K111、K11、K1、KRを所有する。なお、図11のツリーにはデバイスが0~15の16個のみ記載され、ツリー構造も4段構成の均衡のとれた左右対称構成として示しているが、さらに多くのデバイスがツリー中に構成され、また、ツリーの各部において異なる段数構成を持つことが可能である。

【0126】また、図11のツリー構造に含まれる各記録再生器には、様々な記録媒体、例えばDVD、CD、MD、メモリスティック(商標)等を使用する様々なタイプの記録再生器が含まれている。さらに、様々なアプリケーションサービスが共存することが想定される。このような異なるデバイス、異なるアプリケーションの共存構成の上に図11に示すキー配布構成が適用されている。

【0127】これらの様々なデバイス、アプリケーションが共存するシステムにおいて、例えば図11の点線で囲んだ部分、すなわちデバイス0、1、2、3を同一の記録媒体を用いるひとつのグループとして設定する。例えば、この点線で囲んだグループ内に含まれるデバイスに対しては、まとめて、共通のコンテンツを暗号化してプロバイダから送付したり、共通に使用するマスターキーを送付したり、あるいは各デバイスからプロバイダあるいは決済機関等にコンテンツ料金の支払データをやはり暗号化して出力するといった処理が実行される。コンテンツプロバイダ、あるいは決済処理機関等、各デバイスとのデータ送受信を行なう機関は、図11の点線で囲んだ部分、すなわちデバイス0、1、2、3を1つのグループとして一括してデータを送付する処理を実行する。このようなグループは、図11のツリー中に複数存在する。

【0128】なお、ノードキー、リーフキーは、ある1つの鍵管理センタによって統括して管理してもよいし、各グループに対する様々なデータ送受信を行なうプロバイダ、決済機関等によってグループごとに管理する構成としてもよい。これらのノードキー、リーフキーは例えばキーの漏洩等の場合に更新処理が実行され、この更新処理は鍵管理センタ、プロバイダ、決済機関等が実行する。

【0129】このツリー構成において、図11から明らかなように、1つのグループに含まれる3つのデバイス0、1、2、3はノードキーとして共通のキーK00、K0、KRを保有する。このノードキー共有構成を利用することにより、例えば共通のマスターキーをデバイス0、1、2、3のみに提供することが可能となる。たとえば、共通に保有するノードキーK00自体をマスターキーとして設定すれば、新たな鍵送付を実行することなくデバイス0、1、2、3のみが共通のマスターキーの

設定が可能である。また、新たなマスターキー Kmaster をノードキー K00 で暗号化した値 Enc (K00, Kmaster) を、ネットワークを介してあるいは記録媒体に格納してデバイス 0, 1, 2, 3 に配布すれば、デバイス 0, 1, 2, 3 のみが、それぞれのデバイスにおいて保有する共有ノードキー K00 を用いて暗号 Enc (K00, Kmaster) を解いてマスターキー: Kmaster を得ることが可能となる。なお、Enc (Ka, Kb) は Kb を Ka によって暗号化したデータであることを示す。

【0130】また、ある時点 t において、デバイス 3 の所有する鍵: K0011, K001, K00, K0, KR が攻撃者 (ハッカー) により解析されて露呈したことが発覚した場合、それ以降、システム (デバイス 0, 1, 2, 3 のグループ) で送受信されるデータを守るために、デバイス 3 をシステムから切り離す必要がある。そのためには、ノードキー: K001, K00, K0, KR をそれぞれ新たな鍵 K(t)001, K(t)00, K(t)0, K(t)R に更新し、デバイス 0, 1, 2 にその更新キーを伝える必要がある。ここで、K(t)aaa は、鍵 Kaaa の世代 (Generation): t の更新キーであることを示す。

【0131】更新キーの配布処理について説明する。キーの更新は、例えば、図 12 (A) に示す有効化キープブロック (EKB: Enabling Key Block) と呼ばれるブロックデータによって構成されるテーブルをたとえばネットワーク、あるいは記録媒体に格納してデバイス 0, 1, 2 に供給することによって実行される。

【0132】図 12 (A) に示す有効化キープブロック (EKB) には、ノードキーの更新に必要なデバイスのみが更新可能なデータ構成を持つブロックデータとして構成される。図 12 の例は、図 11 に示すツリー構造中のデバイス 0, 1, 2 において、世代 t の更新ノードキーを配布することを目的として形成されたブロックデータである。図 11 から明らかなように、デバイス 0, デバイス 1 は、更新ノードキーとして K(t)00, K(t)0, K(t)R が必要であり、デバイス 2 は、更新ノードキーとして K(t)001, K(t)00, K(t)0, K(t)R が必要である。

【0133】図 12 (A) の EKB に示されるように EKB には複数の暗号化キーが含まれる。最下段の暗号化キーは、Enc (K0010, K(t)001) である。これはデバイス 2 の持つリーフキー K0010 によって暗号化された更新ノードキー K(t)001 であり、デバイス 2 は、自身の持つリーフキーによってこの暗号化キーを復号し、K(t)001 を得ることができる。また、復号により得た K(t)001 を用いて、図 12 (A) の下から 2 段目の暗号化キー Enc (K(t)001, K(t)00) を復号可能となり、更新ノードキー K(t)00 を得ることができる。以下順次、図 12 (A) の上から 2 段目の暗号化キー Enc

(K(t)00, K(t)0) を復号し、更新ノードキー K(t)0、図 12 (A) の上から 1 段目の暗号化キー Enc (K(t)0, K(t)R) を復号し K(t)R を得る。一方、デバイス 0, 1 は、ノードキー K00 は更新する対象に含まれておらず、更新ノードキーとして必要なのは、K(t)00, K(t)0, K(t)R である。デバイス 0, 1 は、図 12 (A) の上から 3 段目の暗号化キー Enc (K000, K(t)00) を復号し K(t)00 を取得し、以下、図 12 (A) の上から 2 段目の暗号化キー Enc (K(t)00, K(t)0) を復号し、更新ノードキー K(t)0、図 12 (A) の上から 1 段目の暗号化キー Enc (K(t)0, K(t)R) を復号し K(t)R を得る。このようにして、デバイス 0, 1, 2 は更新した鍵 K(t)R を得ることができる。なお、図 12 (A) のインデックスは、復号キーとして使用するノードキー、リーフキーの絶対番地を示す。

【0134】図 11 に示すツリー構造の上位段のノードキー: K0, KR の更新が不要であり、ノードキー K0 のみの更新処理が必要である場合には、図 12 (B) の有効化キープブロック (EKB: Enabling Key Block) を用いることで、更新ノードキー K(t)00 をデバイス 0, 1, 2 に配布することができる。

【0135】図 12 (B) に示す EKB は、例えば特定のグループにおいて共有する新たなマスターキーを配布する場合に利用可能である。具体例として、図 11 に点線で示すグループ内のデバイス 0, 1, 2, 3 がある記録媒体を用いており、新たな共通のマスターキー K(t)master が必要であるとする。このとき、デバイス 0, 1, 2, 3 の共通のノードキー K00 を更新した K(t)00 を用いて新たな共通の更新マスターキー: K(t)master を暗号化したデータ Enc (K(t), K(t)master) を図 12 (B) に示す EKB とともに配布する。この配布により、デバイス 4 など、その他のグループの機器においては復号されないデータとしての配布が可能となる。

【0136】すなわち、デバイス 0, 1, 2 は EKB を処理して得た K(t)00 を用いて上記暗号文を復号すれば、t 時点でのマスターキー K(t)master を得ることが可能になる。

【0137】[EKB を使用したマスターキーの配布] 図 13 に、t 時点でのマスターキー K(t)master を得る処理例として、K(t)00 を用いて新たな共通のマスターキー K(t)master を暗号化したデータ Enc (K(t)00, K(t)master) と図 12 (B) に示す EKB とを記録媒体を介して受領したデバイス 0 の処理を示す。

【0138】図 13 に示すように、デバイス 0 は、記録媒体に格納されている世代: t 時点の EKB と自分があらかじめ格納しているノードキー K000 を用いて上述

したと同様のEKB処理により、ノードキー $K(t)0$ を生成する。さらに、復号した更新ノードキー $K(t)00$ を用いて更新マスターキー $K(t)master$ を復号して、後にそれを使用するために自分だけが持つリーフキー $K0000$ で暗号化して格納する。なお、デバイス0が更新マスターキー $K(t)master$ を安全に自身内に格納できる場合、リーフキー $K0000$ で暗号化する必要はない。

【0139】また、この更新マスターキーの取得処理を図14のフローチャートにより説明する。なお、記録再生装置は出荷時にその時点で最新のマスターキー:

(c) masterを与えられ、自身のメモリに安全に(具体的にはたとえば、自身のリーフキーで暗号化して)格納しているものとする。

【0140】更新マスターキー $K(n)master$ とEKBの格納された記録媒体が、記録再生装置にセットされると、まず最初に、ステップS1401において、記録再生装置は、記録媒体から、記録媒体に格納されているマスターキー $K(n)master$ の時点(世代)番号: $n$ (これを、プレ(pre-recording)記録世代情報(Generation# $n$ )と呼ぶことにする)を読み出す。記録媒体には、予め、マスターキー $K(n)master$ の時点(世代)番号: $n$ が記憶されている。また、自身が保持している暗号化マスターキーCを読み出し、ステップS1402において、その暗号化マスターキーの世代: $c$ と、プレ記録世代情報Generation# $n$ が表す世代: $n$ とを比較して、その世代の前後を判定する。

【0141】ステップS1402において、プレ記録世代情報Generation# $n$ が表す世代: $n$ の方が、自身のメモリに記憶された暗号化マスターキーCの世代: $c$ よりも後でない(新しくない)と判定された場合、即ち、メモリに記憶された暗号化マスターキーCの世代: $c$ が、プレ記録世代情報Generation# $n$ が表す世代: $n$ と同一か、または後の場合、ステップS1403乃至S1408をスキップして、マスターキー更新処理を終了する。即ち、この場合、自身のメモリに記憶されたマスターキー $K(c)master$ (暗号化マスターキーC)の更新は行う必要がないので、その更新は行われない。

【0142】一方、ステップS1402において、プレ記録世代情報Generation# $n$ が表す世代: $n$ の方が、メモリに記憶された暗号化マスターキーCの世代: $c$ よりも後である(新しい)と判定された場合、即ち、メモリに記憶された暗号化マスターキーCの世代が、プレ記録世代情報Generation# $n$ が表す世代 $n$ よりも前の世代である場合、ステップS1403に進み、記録再生装置は、記録媒体から、有効化キープブロック(EKB:Enabling Key Block)を読み出す。

【0143】ステップS1404において、記録再生装置は、ステップS1403で読み出したEKBと、自身がメモリに格納しているリーフキー(図11のデバイス

0における $K0000$ )およびノードキー(図11のデバイス0における $K000, K00\dots$ )を用いて、プレ記録世代情報Generation# $n$ (図13における $t$ )時点でのノード00の鍵 $K(t)00$ を計算する。

【0144】ステップS1405では、ステップS1404において $K(t)00$ を得られたか否かを検査する。得られなかった場合は、その時点においてその記録再生装置がツリー構成のグループからリボーク(排除)されていることを示すので、ステップS1406乃至S1408をスキップしてマスターキー更新処理を終了する。

【0145】 $K(t)00$ を得られた場合、ステップS1406に進み、記録媒体からEnc( $K(t)00, K(t)master$ )、すなわち、 $K(t)00$ を用いて $t$ 時点でのマスターキーを暗号化した値を読み出す。そしてステップS1407において、この暗号文を $K(t)00$ を用いて復号して $K(t)master$ を計算する。

【0146】ステップS1408では、自身のみが持つリーフキー(図11のデバイス0における $K0000$ )を用いて $K(t)master$ を暗号化してメモリに格納する。以上で、マスターキーの更新処理が完了する。

【0147】ところで、マスターキーは、時点(世代)0から昇順に使用されていくが、新しい世代のマスターキーから、古い世代のマスターキーを計算によりシステム内の各機器が求められる構成とすることが望ましい。すなわち、記録再生装置は、一方向性関数 $f$ を保持しており、その一方向性関数 $f$ に、自身が持つマスターキーを、そのマスターキーの世代と、必要なマスターキーの世代との差に対応する回数だけ適用することにより、調べた世代のマスターキーを作成する。

【0148】具体的には、例えば、記録再生装置に記憶されているマスターキーMKの世代が世代 $i+1$ であり、あるデータの再生に必要な(記録時に使用された)マスターキーMKの世代が世代 $i-1$ である場合、マスターキー $K(i-1)master$ は、記録再生装置において、一方向性関数 $f$ が2回用いられ、 $f(f(K(i+1)master))$ を計算することにより生成される。

【0149】また、記録再生装置に記憶されているマスターキーの世代が世代 $i+1$ であり、必要なマスターキーの世代が世代 $i-2$ である場合、マスターキー $K(i-2)master$ は、一方向性関数 $f$ を3回用いて、 $f(f(f(K(i+1)master)))$ を計算することにより生成される。

【0150】ここで、一方向性関数としては、例えば、ハッシュ(hash)関数を用いることができる。具体的には、例えば、MD5(Message Digest 5)や、SHA-1(Secure Hash Algorithm-1)等を採用することができる。キーを発行するキー発行機関は、これらの一方向性関数を用いて自身の世代より前の世代を生成可能なマスターキー $K(0)master, K(1)master, K(2)ma$

sfer . . . , K ( N ) master を、あらかじめ求めておく。即ち、まず最初に、第 N 世代のマスターキー K ( N ) master を設定し、そのマスターキー K ( N ) master に、一方向性関数を 1 回ずつ適用していくことで、それより前の世代のマスターキー K ( N - 1 ) master, K ( N - 2 ) master, . . . , K ( 1 ) master, K ( 0 ) master を順次生成しておく。そして、世代の小さい ( 前 ) のマスターキー K ( 0 ) master から順番に使用していく。なお、自身の世代より前の世代のマスターキーを生成するのに用いる一方向性関数は、すべての記録再生装置に設定されているものとする。

【 0151 】 また、一方向性関数としては、例えば、公開鍵暗号技術を採用することも可能である。この場合、キー発行機関は、公開鍵暗号方式の秘密鍵を所有し、その秘密鍵に対する公開鍵を、すべての再生装置に与えておく。そして、キー発行機関は、第 0 世代のマスターキー K ( 0 ) master を設定し、そのマスターキー K ( 0 ) master から使用していく。即ち、キー発行機関は、第 1 世代以降のマスターキー K ( i ) master が必要になったら、その 1 世代前のマスターキー K ( i - 1 ) master を、秘密鍵で変換することにより生成して使用する。この場合、キー発行機関は、一方向性関数を用いて、N 世代のマスターキーを、あらかじめ生成しておく必要がない。また、この方法によれば、理論上は、無制限の世代のマスターキーを生成することができる。なお、記録再生装置では、ある世代のマスターキーを有していれば、そのマスターキーを、公開鍵で変換することにより、その世代より前の世代のマスターキーを得ることができる。

【 0152 】 次に、この記録再生装置がコンテンツを自身の記録媒体に記録する場合の、記録再生装置の処理について図 15 のフローチャートを用いて説明する。コンテンツデータは、ある世代のマスターキーにより暗号化されてネットワークあるいは記録媒体を介してコンテンツプロバイタから各記録再生装置に配布される。

【 0153 】 まず最初に、ステップ S 1501 において、記録再生装置は、記録媒体から、プレ記録世代情報 Generation#n を読み出す。また、自身のメモリが記憶している暗号化マスターキー C の世代 c を取得し、ステップ S 1502 において、その暗号化マスターキーの世代 c と、プレ記録世代情報 Generation#n が表す世代 n とを比較して、その世代の前後を判定する。

【 0154 】 ステップ S 1502 において、メモリに記憶された暗号化マスターキー C の世代 c が、プレ記録世代情報 Generation#n が表す世代 n 以後でないと判定された場合、即ち、メモリに記憶された暗号化マスターキー C の世代 c が、プレ記録世代情報 Generation#n が表す世代 n よりも古い世代である場合、ステップ S 1503 をスキップして、すなわち、コンテンツデータの記録処理を行わずに終了する。

【 0155 】 一方、ステップ S 1502 において、自身の記録再生装置内のメモリに記憶された暗号化マスターキー C の世代が、プレ記録世代情報 Generation#n が表す世代 n 以後であると判定された場合、即ち、メモリに記憶された暗号化マスターキー C の世代が、プレ記録世代情報 Generation#n が表す世代 n と同一か、またはそれよりも新しい場合、ステップ S 1503 に進み、コンテンツデータの記録処理を行う。

【 0156 】 [ 世代管理のなされたマスターキーによるコンテンツデータ暗号化および記録処理 ] 以下、世代管理のなされたマスターキーによってコンテンツデータの暗号化処理を実行して、自己の記録媒体に格納する処理について説明する。なお、ここでは、先に説明したトランスポートストリームによって構成されるデータを世代管理されたマスターキーを利用したデータに基づいてブロックキーを生成してブロックキーによりコンテンツデータを暗号化して記録媒体に格納する処理について説明する。

【 0157 】 図 16、図 17 の処理ブロック図および図 18 のフローチャートを用いて説明する。ここでは、記録媒体として光ディスクを例とする。この実施例では、記録媒体上のデータの bit-by-bit コピーを防ぐために、記録媒体固有の識別情報としてのディスク ID ( Disc ID ) を、データを暗号化する鍵に作用させるようにしている。

【 0158 】 図 16、図 17 の処理ブロック図に従って、暗号処理手段 150 が実行するデータの暗号化処理の概要について説明する。

【 0159 】 記録再生装置 1600 は自身のメモリ 180 ( 図 1、2 参照 ) に格納しているマスターキー 1601、データ解析記録方式用キー ( コグニザントキー : Cognizant Key ) 1631 もしくはデータ非解析記録方式用キー ( ノンコグニザントキー : Non-Cognizant Key ) 1632 を読み出す。データ解析記録方式用キー ( Cognizant Key )、データ非解析記録方式用キー ( Non-Cognizant Key ) については、後述する。

【 0160 】 マスターキー 1601 は、図 14 のフローにより記録再生装置のメモリに格納された秘密キーであり、前述のように世代管理がなされており、それぞれに世代番号が対応付けられている。このマスターキーは、複数の記録再生装置に共通なキー、例えば図 11 に示す点線枠のグループに属するデバイスに共通なキーである。デバイス ID は記録再生装置 1600 の識別子であり、予め記録再生装置に格納されている例えば製造番号等の識別子である。このデバイス ID は公開されていてもよい。データ解析記録方式用キー ( Cognizant Key ) 1631、データ非解析記録方式用キー ( Non-Cognizant Key ) 1632 は、それぞれの記録モードに対応したキーであり、複数の記録再生装置に共通のキーである。

これらは予め記録再生装置 1600 のメモリに格納され

ている。

【0161】記録再生装置1600は例えば光ディスクである記録媒体1620に識別情報としてのディスクID (Disc ID) 1603が既に記録されているかどうかを検査する。記録されていれば、ディスクID (Disc ID) 1603を読み出し (図16に相当)、記録されていなければ、暗号処理手段150においてランダムに、もしくはあらかじめ定められた例えば乱数発生等の方法でディスクID (Disc ID) 1701を生成し、ディスクに記録する (図17に相当)。ディスクID (Disc ID) 1603はそのディスクにひとつあればよいので、リードインエリアなどに格納することも可能である。

【0162】記録再生器1600は、次にマスターキーと、特殊な読み取り方法でのみディスクから読み取り可能な秘密情報として記録されたスタンパーID (Stamper ID) 1680と、ディスクID 1603を用いて、ディスク固有キー (Disc Unique Key) を生成1602する。

【0163】マスターキーと秘密情報としてのスタンパーID (Stamper ID) 1680とディスクID 1603とを用いディスク固有キー (Disc Unique Key) の具体的な生成方法としては、図19に示すように、ブロック暗号関数を用いたハッシュ関数にマスターキー (Master Key) とスタンパーID (Stamper ID) とディスクID (Disc ID) を入力して得られた結果を用いる例1の方法や、FIPS 180-1で定められているハッシュ関数SHA-1に、マスターキーとスタンパーID (Stamper ID) とディスクID (Disc ID) とのビット連結により生成されるデータを入力し、その160ビットの出力から必要なデータ長のみをディスク固有キー (Disc Unique Key) として使用する例2の方法が適用できる。

【0164】上述したように、スタンパーID (Stamper ID) 1680は、あらかじめディスクに記録されている高度な秘密情報であり、その読み出しおよび読み出されたスタンパーID (Stamper ID) を利用したディスク固有キー (Disc Unique Key) の生成などの演算処理は、秘密が保たれるように暗号処理手段内部で実行される。すなわち、ディスクから読み出された秘密情報は暗号処理手段内においてセキュアに保護される。

【0165】このように、本発明の構成においては、特殊の読み出し方法でのみ読み取り可能な秘密情報は、正当なデバイス、すなわち秘密情報の読み取り方法を実行可能なデバイスでのみ読み取られ、たとえばLSI内に実装されて高度に保護された暗号鍵の生成を実行する暗号処理部においてセキュアな保護の下にコンテンツ暗号処理用の鍵生成処理に使用される構成であり、秘密情報が外部からの読み取り可能なメモリ上に格納されない。従って、秘密情報の漏洩の可能性がなく、不正なコンテンツの再生処理を効果的に防止することが可能となる。

【0166】上述したように、スタンパーID等の秘密

情報は、通常のデータ書き込み手法とは異なる態様でディスクに書き込まれ、また、通常のデータ読み出しとは、異なる手法でのみ読み取り可能である。この秘密情報の書き込みおよび読み出し処理構成例については後段で詳細に説明する。

【0167】記録再生装置1600は、次に、記録ごとの固有鍵であるタイトルキー (Title Key) を暗号処理手段150 (図1, 2, 参照) においてランダムに、もしくはあらかじめ定められた例えば乱数発生等の方法で生成1604し、ディスク1620に記録する。

【0168】さらに、この記録における記録モードがデータ解析記録方式 (Cognizant Mode) かデータ非解析記録方式 (Non-cognizant) かを表すフラグを設定1633し、ディスク1620に記録モード1635を記録する。

【0169】ここで、データ解析記録方式 (Cognizant Mode) およびデータ非解析記録方式 (Non-Cognizant Mode) について説明する。

【0170】コンテンツはそれぞれあらかじめコンテンツ提供者によっていかなる条件で複製が可能かを指定されている。そこで、ネットワーク接続においてもその指定された条件を正しく相手の機器に伝える必要性があり、企業5社の共同提案としての5C D T C P (Digital Transmission Content Protection) システムではコピー制御情報 (CCI : Copy Control Information) という方法を用いて解決している。コピー制御情報 (CCI) はデバイスの能力に応じて2種類の伝達方法が規定されている。

【0171】エンクリプションモード・インディケータ (EMI : Encryption Mode Indicator) はパケットヘッダにあるSyビットの上位2ビットを使ってコピー制御情報 (CCI) を送るメカニズムであり、受信デバイスが簡単にアクセスする事ができると同時に、この値がコンテンツを暗号化する鍵に作用するため安全に送ることができるになっている。

【0172】EMIによりそのパケットの暗号化モードを示し、コンテンツ暗号・復号鍵の生成モードを指定する。EMIをIEEE1394パケットヘッダに置くことにより、受信機器は例えばMPEG転送ストリーム (MPEG Transport stream) の中に埋め込まれている埋め込みコピー制御情報 (Embedded CCI) (後述) を取り出すことなく簡単にどのモードでコンテンツが暗号化されているかを知ることがでる。

【0173】図20にIEEE1394パケットフォーマットを示す。データフィールド (Data Field) 中には、音楽データ、画像データ等、様々なコンテンツが格納され、コピー制御情報 (CCI) としてのエンクリプション・モード・インディケータ (EMI : Encryption Mode Indicator) はパケットヘッダにあるSyビットの上位2ビットに設定される。

【0174】EMIの2ビット情報は、設定値に応じてコンテンツの異なる取り扱いを規定する。具体的には、値00は認証も暗号化も必要がなく、コンテンツは自由にコピーが可能なコピーフリー(Copy Free)を示し、値01は一世代コピーの作成が可能なコピー1ジェネレーション(Copy One Generation)を、値10は前述のCopy One Generationが一度記録された後の、再コピーが禁止されているノーモアコピー(No More Copies)を、値11はコンテンツがリリース時点からコピー禁止であるネバーコピー(Never Copy)を表す。

【0175】D-VHSやハードディスクのような記録されるデータのフォーマットを認識しないようなビットストリームレコーダでも正しく著作物を取り扱えるように、記録時に埋め込みCCI(Embedded CCI)の更新(ex. Copy One GenerationからNo More Copiesへ)を必要とせず、EMIの更新のみ行えばよい、という記録方法がデータ非解析(Non-Cognizant)記録方式である。

【0176】一方、こういったコピー制御情報を送るための場所があらかじめ確保されているようなフォーマット(たとえばDVフォーマット:DV-format)においては、CCIはコンテンツの一部として伝送することができる。このように、コンテンツの一部としてコンテンツに埋め込まれたコピー制御情報(CCI)を埋め込みCCI(Embedded CCI)と呼ぶ。通常、コンテンツが暗号化されて転送される場合、埋め込みCCI(Embedded CCI)もコンテンツと同様に暗号化されて転送され、埋め込みCCI(Embedded CCI)の故意の変更は困難とされている。

【0177】ここで、前述したEMIの2ビットのコピー制御情報と、埋め込みCCI(Embedded CCI)との双方を持つコンテンツの場合、コンテンツ記録を実行するある記録デバイスは、EMIおよび埋め込みCCI(Embedded CCI)の双方のコピー制御情報の更新を行なう。しかし、埋め込みCCI(Embedded CCI)の解析能力のない記録デバイスの場合、EMIは更新するが、埋め込みCCI(Embedded CCI)の更新は実行しないことになる。

【0178】コンテンツ記録時に、記録デバイスがコンテンツの一部として伝送された埋め込みCCI(Embedded CCI)の更新を行ってコンテンツとともに記録する記録方式をデータ解析(Cognizant)記録方式という。データ解析(Cognizant)記録方式と、データ非解析(Non-Cognizant)記録方式では、データ非解析(Non-Cognizant)記録方式の方が埋め込みCCI(Embedded CCI)の更新を行わなくてよい分、負荷が軽く実装しやすいが、5C D T C Pのルールとして、その機器がコンテンツをM P E Gデコードしてアナログ端子から映像信号を表示するためにはその機器はデータ解析記録方式(Cognizant Mode)でなければならないというルールがあり、デコー

ド/表示機能を持つ機器はデータ解析記録方式(Cognizant Mode)を実行する機能を備えていることが必要である。

【0179】しかしまた、データ解析記録方式(Cognizant Mode)を実行するためには、コンテンツの一部として埋め込まれている埋め込みCCI(Embedded CCI)の位置や意味を完全に知る必要があり、たとえばある機器が市場に出た後に制定された新規のあるいは更新されたデータフォーマットについては、その新しいデータフォーマットに対して、古い機器がデータ解析記録方式(Cognizant Mode)を実行するのは非常に困難となる場合がある。

【0180】従って、コンテンツを記録するある機器が、特定のデータフォーマットについては、もしくは、特定の機能を実現するときには、データ解析記録方式(Cognizant Mode)を実行し、また異なるデータフォーマットのコンテンツ記録時には、データ非解析記録方式(Non-Cognizant Mode)を実行するといった、両方の記録方式を実行することが考えられる。

【0181】また、すべてのコンテンツに対して、データ非解析記録方式(Non-Cognizant Mode)の記録しか行わない機器も存在する。また、逆に埋め込みCCI(Embedded CCI)を理解できるフォーマットを持つコンテンツの処理しか実行しない機器、すなわちデータ解析記録方式(Cognizant Mode)のみ実行する機器も存在することが考えられる。

【0182】このように、2つのコピー制御情報、すなわちEMIと埋め込みCCI(Embedded CCI)が存在し、またコンテンツ記録を実行する機器としても、データ解析記録方式(Cognizant Mode)を実行する機器と、データ非解析記録方式(Non-Cognizant Mode)の記録を実行する機器が混在する状況においては、データ解析記録方式(Cognizant Mode)で記録したコンテンツと、データ非解析記録方式(Non-Cognizant Mode)で記録したコンテンツは明確に区別されることが好ましい。

【0183】すなわち、データ解析記録方式(Cognizant Mode)でコンテンツを記録した場合にはEMIも埋め込みCCI(Embedded CCI)の双方のコピー制御情報が更新されるが、データ非解析記録方式(Non-Cognizant Mode)でコンテンツの記録が実行された場合は、EMIのみが更新され、埋め込みCCI(Embedded CCI)の更新が行なわれない。その結果、記録媒体上のEMIと埋め込みCCI(Embedded CCI)に不整合がおり、その両者が混ざると混乱が生じるためである。従って、2つのコピー制御情報の不整合を発生させないためには、データ解析記録方式(Cognizant Mode)で記録されたコンテンツは、データ解析記録方式(Cognizant Mode)モードでの記録再生処理を実行し、データ非解析記録方式(Non-Cognizant Mode)で記録されたコンテンツはデータ非解析記録方式(Non-Cognizant Mode)モードで記録

再生処理を実行する構成とすることが必要となる。

【0184】このためには、このデータ解析記録方式 (Cognizant Mode) と、データ非解析記録方式 (Non-Cognizant Mode) とをまったく別の記録方式とすることも一案ではあるが、この場合、1つの機器において両方のモードを選択的に実行可能とするためには、1機器に両モードの実行処理構成を装備することが必要となり、これは、機器のコスト高を招くという問題がある。

【0185】そこで本発明の構成では、この2つの記録方式、すなわちデータ解析記録方式 (Cognizant Mode) と、データ非解析記録方式 (Non-Cognizant Mode) のいずれの方式を適用するかに応じて、コンテンツ暗号処理用の鍵を異なる鍵として生成して使用する構成とすることで、機器および記録方式に応じて2つの記録方式を明確に区別して、両方式が無秩序に混在して実行される事態を解消し、機器および記録方式に応じたいずれか一方の統一的な記録方式によるコンテンツ処理構成を、機器の装備および処理負荷を増大させることなく実現したものである。

【0186】具体的には、データ解析記録方式 (Cognizant Mode) 記録用の秘密情報 (再生時にも必要) としての暗号化、復号処理鍵生成用のキー (データ解析記録方式用キー (Cognizant Key)) をデータ解析記録方式 (Cognizant Mode) による記録または再生を行える機能を持つ機器にのみ提供して機器内に格納する構成とし、一方、データ非解析記録方式 (Non-Cognizant Mode) 記録用の秘密情報 (再生時にも必要) としての暗号化、復号処理鍵生成用のキー (データ非解析記録方式用キー (Non-Cognizant Key)) を、データ非解析記録方式 (Non-Cognizant Mode) による記録または再生を行える機能を持つ機器にのみ提供して機器内に格納する構成とした。

【0187】本構成により、例えば、データ解析記録方式 (Cognizant Mode) で記録されたコンテンツについて、バグを原因として、あるいはデータの改竄、記録再生プログラムの不正改造等によって、データ非解析記録方式 (Non-Cognizant Mode) の記録再生機能のみを有する機器において、誤ってまたは不正な記録再生の実行を防止することができる。

【0188】図16、図17に戻って、コンテンツ記録処理の説明を続ける。記録再生装置1600は、さらに、使用するマスターキーの世代番号、すなわち、自身が格納するマスターキーの世代番号 [記録時世代番号 (Generation#n)] 1650を取得して、これを記録媒体1620に記録時世代番号1651として格納する。

【0189】ディスク上には、どこのデータがどんなタイトルを構成するかという情報が格納されたデータ管理ファイルがあり、このファイルにタイトルキー1605、記録モードフラグ1635、マスターキーの世代番号 [記録時世代番号 (Generation#n)] 1651を格納することができる。

【0190】なお、記録媒体1620には、予め、プレ (pre-recording) 世代番号が格納されており、プレ世代番号と同一またはプレ世代番号より新しい世代のマスターキーを用いて暗号化されて格納されたコンテンツのみの再生を可能とする構成となっている。この構成については、後段の再生処理の欄で説明する。

【0191】次にディスク固有キー (Disc Unique Key) とタイトルキー (Title Key) と、データ解析記録方式用キー (Cognizant Key)、あるいは、ディスク固有キー (Disc Unique Key) とタイトルキー (Title Key) と、データ非解析記録方式用キー (Non-Cognizant Key)、いずれかの組合せから、タイトル固有キー (Title Unique Key) を生成する。

【0192】すなわち、記録モードがデータ解析記録方式 (Cognizant Mode) である場合には、ディスク固有キー (Disc Unique Key) とタイトルキー (Title Key) と、データ解析記録方式用キー (Cognizant Key) とからタイトル固有キー (Title Unique Key) を生成し、記録モードがデータ非解析記録方式 (Non-Cognizant Mode) である場合には、ディスク固有キー (Disc Unique Key) とタイトルキー (Title Key) と、データ非解析記録方式用キー (Non-Cognizant Key) とからタイトル固有キー (Title Unique Key) を生成する。

【0193】前述したように、データ解析記録方式 (Cognizant Mode) 記録用の秘密情報としての暗号化、復号処理鍵生成用のキー (データ解析記録方式用キー (Cognizant Key)) は、データ解析記録方式 (Cognizant Mode) による記録または再生を行える機能を持つ機器のみが有し、一方、データ非解析記録方式 (Non-Cognizant Mode) 記録用の秘密情報としての暗号化、復号処理鍵生成用のキー (データ非解析記録方式用キー (Non-Cognizant Key)) は、データ非解析記録方式 (Non-Cognizant Mode) による記録または再生を行える機能を持つ機器のみが有する。従って、一方の記録方式にのみ対応した機器においては、いずれか一方のモードのみを選択してコンテンツ記録が実行される。すなわち、データ解析記録方式用キー (Cognizant Key) を用いるか、あるいはデータ非解析記録方式用キー (Non-Cognizant Key) を用いるかの一方のみに限られることとなる。

【0194】しかし、両者のキーを格納し、両モードの記録方式を実行可能な機器においては、いずれのモードによる記録を実行するかを決定する処理が必要となる。このモード決定プロセス処理について、すなわち、コンテンツの記録をデータ解析記録方式 (Cognizant Mode) によって実行するか、データ非解析記録方式 (Non-Cognizant Mode) で実行するかを決定するプロセスについて図21を用いて説明する。

【0195】基本的には、コンテンツ記録は、できる限りデータ解析記録方式 (Cognizant Mode) によって実行するのが望ましい。これは、前述したように、EMIと埋

め込みCCI (Embedded CCI) との不整合を生じさせないためである。ただし、前述したように、新規なデータフォーマットの出現等によるデータ解析エラー等の発生の可能性もあり、このような場合に、データ非解析記録方式 (Non-Cognizant Mode)での記録処理を実行する。

【0196】図21の各ステップについて説明する。ステップS5001では、記録装置は、データ・フォーマットを解析可能か否かを判定する。先に説明したように、埋め込みCCI (Embedded CCI) は、コンテンツの内部に埋め込まれており、データフォーマットの解析が不可能であれば、埋め込みCCI (Embedded CCI) の読み取りが不可能となるので、この場合は、データ非解析記録方式 (Non-Cognizant Mode)での記録処理を実行する。

【0197】データフォーマットの解析が可能であれば、ステップS5002に進み、記録装置が、データ (コンテンツ) のデコード処理、埋め込みCCI (Embedded CCI) の読み取り、更新処理が可能か否かを判定する。コンテンツおよび埋め込みCCI (Embedded CCI) は通常、符号化 (エンコード) されており、埋め込みCCI (Embedded CCI) の読み取りには復号 (デコード) を実行することが必要となる。例えば多チャンネル同時記録などの際に、復号回路が他に使用されているなど理由で、機器が復号処理可能でない場合は、埋め込みCCI (Embedded CCI) の読み取りができないので、データ非解析記録方式 (Non-Cognizant Mode)での記録処理を実行する。

【0198】ステップS5002のデータ (コンテンツ) のデコード処理、埋め込みCCI (Embedded CCI) の読み取り、更新処理が可能であると判定されると、ステップS5003において、記録装置に対するユーザ入力中に、データ非解析モードでの記録処理の実行指定入力があるか、否かが判定される。この処理は、ユーザの指定によるモード選択を可能とした機器においてのみ実行されるステップであり、通常の機器、すなわちユーザによるモード指定を許容しない機器においては実行されない。ユーザ入力によるデータ非解析記録方式 (Non-Cognizant Mode)での記録処理指定があった場合は、データ非解析記録方式 (Non-Cognizant Mode)での記録処理が実行される。

【0199】次に、ステップS5004において、コンテンツパケット (ex. 受信データ) 中に、データ非解析モードでの記録処理の実行指定があるか否かが判定される。データ中にデータ非解析モードでの記録処理の実行指定がある場合は、データ非解析記録方式 (Non-Cognizant Mode)での記録処理が実行される。指定がない場合は、データ解析記録方式 (Cognizant Mode)での記録処理が実行される。

【0200】データ解析記録方式 (Cognizant Mode)での記録処理、およびデータ非解析記録方式 (Non-Cogniz

ant Mode)での記録処理の双方を選択的に実行可能な機器においては、上述したモード決定プロセス処理によって、いずれのモードでの記録を実行するかが決定される。ただし、図21の処理フローからも理解されるように、データ解析記録方式 (Cognizant Mode)での記録が可能な場合は、基本的にデータ解析記録方式 (Cognizant Mode)での処理が実行されることになる。

【0201】前述したように、記録モードをデータ解析記録方式 (Cognizant Mode)とした場合は、ディスク固有キー (Disc Unique Key) とタイトルキー (Title Key) と、データ解析記録方式用キー (Cognizant Key) からタイトル固有キー (Title Unique Key) を生成し、記録モードをデータ非解析記録方式 (Non-Cognizant Mode)とした場合は、ディスク固有キー (Disc Unique Key) とタイトルキー (Title Key) と、データ非解析記録方式用キー (Non-Cognizant Key) とからタイトル固有キー (Title Unique Key) を生成する。

【0202】タイトル固有キー (Title Unique Key) 生成の具体的な方法を図22に示す。図22に示すように、ブロック暗号関数を用いたハッシュ関数にタイトルキー (Title Key) とディスク固有キー (Disc Unique Key) と、データ解析記録方式用キー (Cognizant Key) (データ解析記録方式 (Cognizant Mode)の場合)、もしくは、データ非解析記録方式用キー (Non-Cognizant Key) (データ非解析記録方式 (Non-Cognizant Mode)の場合)を入力して得られた結果を用いる例1の方法、あるいは、FIPS 180-1で定められているハッシュ関数SHA-1に、マスターキーとディスクID (Disc ID) とデータ解析記録方式用キー (Cognizant Key) (データ解析記録方式 (Cognizant Mode)の場合) もしくはデータ非解析記録方式用キー (Non-Cognizant Key) (データ非解析記録方式 (Non-Cognizant Mode)の場合) とのビット連結により生成されるデータを入力し、その160ビットの出力から必要なデータ長のみをタイトル固有キー (Title Unique Key) として使用する例2の方法が適用できる。

【0203】なお、上記の説明では、マスターキー (Master Key) とスタンパーID (Stamper ID) とディスクID (Disc ID) からディスク固有キー (Disc Unique Key) を生成し、これとタイトルキー (Title Key) とデータ解析記録方式用キー (Cognizant Key) もしくはデータ非解析記録方式用キー (Non-Cognizant Key) からタイトル固有キー (Title Unique Key) をそれぞれ生成するようにしているが、ディスク固有キー (Disc Unique Key) を不要としてマスターキー (Master Key) とディスクID (Disc ID) とタイトルキー (Title Key) と、データ解析記録方式用キー (Cognizant Key) もしくはデータ非解析記録方式用キー (Non-Cognizant Key) から直接タイトル固有キー (Title Unique Key) を生成してもよく、また、タイトルキー (Title Key) を用いずに、マ

スターキー (Master Key) とディスク ID (Disc ID) と、データ解析記録方式用キー (Cognizant Key) もしくはデータ非解析記録方式用キー (Non-Cognizant Key) からタイトル固有キー (Title Unique Key) 相当の鍵を生成してもよい。

【0204】たとえば上記の5CDTCPに規定される伝送フォーマットのひとつを使用した場合、データはMPEG2のTSパケットで伝送される場合がある。たとえば、衛星放送を受信したセットップボックス (STB: Set Top Box) がこの放送を記録機に5CDTCPを用いて伝送する際に、STBは衛星放送通信路で伝送されたMPEG2 TSパケットをIEEE1394上にも伝送することが、データ変換の必要がなく望ましい。

【0205】記録再生装置1600は記録すべきコンテンツデータをこのTSパケットの形で受信し、前述したTS処理手段300において、各TSパケットを受信した時刻情報であるATSを付加する。なお、先に説明したように、ブロックデータに付加されるブロック・シードは、ATSとコピー制御情報、さらに他の情報を組み合わせた値から構成してもよい。

【0206】ATSを付加したTSパケットをX個 (例えばX=32) 並べて、1ブロックのブロックデータが形成 (図5の上の図参照) され、図16、17の下段に示すように、被暗号化データとして入力されるブロックデータの先頭の第1~4バイトが分離され (セクタ1608) て出力される32ビットのATSを含むブロックシード (Block Seed) と、先に生成したタイトル固有キー (Title Unique Key) とから、そのブロックのデータを暗号化する鍵であるブロック・キー (Block Key) が生成1607される。

【0207】ブロック・キー (Block Key) の生成方法の例を図23に示す。図23では、いずれも32ビットのブロック・シード (Block Seed) と、64ビットのタイトル固有キー (Title Unique Key) とから、64ビットのブロックキー (Block Key) を生成する例を2つ示している。

【0208】上段に示す例1は、鍵長64ビット、入出力がそれぞれ64ビットの暗号関数を使用している。タイトル固有キー (Title Unique Key) をこの暗号関数の鍵とし、ブロックシード (Block Seed) と32ビットの定数 (コンスタント) を連結した値を入力して暗号化した結果をブロックキー (Block Key) としている。

【0209】例2は、FIPS 180-1のハッシュ関数SHA-1を用いた例である。タイトル固有キー (Title Unique Key) とブロックシード (Block Seed) を連結した値をSHA-1に入力し、その160ビットの出力を、たとえば下位64ビットのみ使用するなど、64ビットに縮約したものをブロックキー (Block Key) としている。

【0210】なお、上記ではディスク固有キー (Disc U

nique key)、タイトル固有キー (Title Unique Key)、ブロックキー (Block Key) をそれぞれ生成する例を説明したが、たとえば、ディスク固有キー (Disc Unique Key) とタイトル固有キー (Title Unique Key) の生成を実行することなく、ブロックごとにマスターキー (Master Key) とスタンパーID (Stamper ID) とディスクID (Disc ID) とタイトルキー (Title Key) とブロックシード (Block Seed) と、データ解析記録方式用キー (Cognizant Key) (Cognizant Mode の場合) もしくはデータ非解析記録方式用キー (Non-Cognizant Key) (データ非解析記録方式 (Non-Cognizant Mode) の場合) を用いてブロックキー (Block Key) を生成してもよい。

【0211】ブロックキーが生成されると、生成されたブロックキー (Block Key) を用いてブロックデータを暗号化する。図16、17の下段に示すように、ブロックシード (Block Seed) を含むブロックデータの先頭の第1~mバイト (たとえばm=8) は分離 (セクタ1608) されて暗号化対象とせず、m+1バイト目から最終データまでを暗号化1609する。なお、暗号化されないmバイト中にはブロック・シードとしての第1~4バイトも含まれる。セクタ1608により分離された第m+1バイト以降のブロックデータは、暗号処理手段150に予め設定された暗号化アルゴリズムに従って暗号化1609される。暗号化アルゴリズムとしては、たとえばFIPS 46-2で規定されるDES (Data Encryption Standard) を用いることができる。

【0212】また、前述したようにブロック・シードには、コピー制限情報 (CCI: Copy Control Information) を含ませることが可能であり、データ解析記録方式 (Cognizant Mode) での記録処理を実行した場合には、コンテンツデータ内部に埋め込まれたコピー制御情報 (CCI) である埋め込みCCI (Embedded CCI) に対応するコピー制御情報が記録され、また、データ非解析記録方式 (Non-Cognizant Mode) での記録処理を実行した場合には、図20で説明したパケットヘッダ上のEMI (Encryption Mode Indicator) を反映したコピー制御情報が記録される。

【0213】すなわち、データ解析記録方式 (Cognizant Mode) による情報記録処理の場合、データ部内の埋め込みコピー制御情報 (CCI) に基づくコピー制御情報を含むブロックシードを、1以上のパケットからなるブロックデータに付加した記録情報生成処理を実行し、データ非解析記録方式 (Non-Cognizant Mode) による情報記録処理の場合、パケットに含まれるコピー制御情報としてのエンクリプション・モード・インディケータ (EMI) に基づくコピー制御情報を含むブロックシードを、1以上のパケットからなるブロックデータに付加した記録情報生成処理を実行する。

【0214】ここで、使用する暗号アルゴリズムのプロ

ック長（入出力データサイズ）がDESのように8バイトであるときは、Xを例えば32とし、mを例えば8の倍数とすることで、端数なくm+1バイト目以降のブロックデータ全体が暗号化できる。

【0215】すなわち、1ブロックに格納するTSパケットの個数をX個とし、暗号アルゴリズムの入出力データサイズをLバイトとし、nを任意の自然数とした場合、 $192 * X = m + n * L$ が成り立つようにX、m、Lを定めることにより、端数処理が不要となる。

【0216】暗号化した第m+1バイト以降のブロックデータは暗号処理のされていない第1～mバイトデータとともにセクタ1610により結合されて暗号化コンテンツ1612として記録媒体1620に格納される。

【0217】以上の処理により、コンテンツはブロック単位で、世代管理されたマスターキー、ATSを含むブロック・シード等に基づいて生成されるブロック鍵で暗号化が施されて記録媒体に格納される。

【0218】上述のように、本構成では、世代管理されたマスターキーによりコンテンツデータが暗号化され記録媒体に格納されているので、その記録媒体を他の記録再生器における再生処理は、少なくとも同一世代、あるいはデータを記録した際に使用されたマスターキーの世代より新しい世代を有する記録再生器であることが復号、すなわち再生可能となる条件となる。

【0219】さらに、ブロックキーは上述のようにデータ解析記録方式 (Cognizant Mode) の記録の場合は、データ解析記録方式用キー (Cognizant Key) に基づいて生成され、データ非解析記録方式 (Non-Cognizant Mode) の記録の場合は、データ非解析記録方式用キー (Non-Cognizant Key) に基づいて生成される。これらの暗号化データは、記録時と同一のモードに対応する鍵（データ解析記録方式用キー (Cognizant Key) もしくはデータ非解析記録方式用キー (Non-Cognizant Key)）を持つ機器でのみ再生可能となる。

【0220】すなわち、データ解析記録方式用キー (Cognizant Key) は、記録時にストリーム中に埋め込まれた Embedded CCI を認識して必要に応じて更新する能力を持つ機器およびそのデータの再生を許された機器にのみ与えられ、この鍵を持たない機器ではデータ解析記録方式 (Cognizant Mode) で記録されたコンテンツの再生は行えない。

【0221】同様に、データ非解析記録方式用キー (Non-Cognizant Key) は、記録時にストリーム中の埋め込みCCI (Embedded CCI) を認識しないデータ非解析記録方式 (Non-Cognizant) の記録モードの機能を持つ機器と、そのモードで記録されたデータの再生を許された機器にのみ与えられ、この鍵を持たない機器ではデータ非解析記録方式 (Non-Cognizant Mode) で記録されたコンテンツの再生は行えないようになっている。なお、再生処理の詳細については後述する。

【0222】次に図18に示すフローチャートに従って、データ記録処理にともなって実行されるTS処理手段300におけるATS付加処理および暗号処理手段150における暗号処理の処理全体の流れをまとめて説明する。図18のS1801において、記録再生装置は自身のメモリ180に格納しているマスターキーおよびデータ解析記録方式用キー (Cognizant Key) (データ解析記録方式 (Cognizant Mode) の場合) もしくはデータ非解析記録方式用キー (Non-Cognizant Key) (データ非解析記録方式 (Non-Cognizant Mode) の場合) を読み出す。また、ディスクからスタンパーID (Stamper ID) を読み出す。

【0223】S1802において、記録媒体に識別情報としてのディスクID (Disc ID) が既に記録されているかどうかを検査する。記録されていればS1803でこのディスクIDを読み出し、記録されていなければS1804で、ランダムに、もしくはあらかじめ定められた方法でディスクIDを生成し、ディスクに記録する。次に、S1805では、マスターキーとスタンパーID (Stamper ID) とディスクIDを用いて、ディスク固有キーを生成する。ディスク固有キーは先に説明したように、例えば、FIPS 180-1で定められているハッシュ関数SHA-1を用いる方法やブロック暗号に基づくハッシュ関数を使用する方法などを適用することで求める。

【0224】次にS1806に進み、その一回の記録ごとの固有の鍵としてのタイトルキー (Title Key) を生成し、記録モード (Recording Mode) とマスターキーの世代番号とともにディスクに記録する。記録モード (Recording Mode) は、実行する情報記録モードが、データ解析記録方式 (Cognizant Mode) であるか、データ非解析記録方式 (Non-Cognizant Mode) であるかを示す。

【0225】次にS1807で、上記のディスク固有キーとタイトルキーと、データ解析記録方式用キー (Cognizant Key) (データ解析記録方式 (Cognizant Mode) の場合) もしくはデータ非解析記録方式用キー (Non-Cognizant Key) (データ非解析記録方式 (Non-Cognizant Mode) の場合) から、タイトル固有キーを生成する。

【0226】タイトル固有キーの生成の詳細フローを図24に示す。暗号処理手段150は、ステップS2001において、記録モードにより分岐する。この分岐は、記録再生器のプログラムや、記録再生器を使用するユーザによって入力された指示データに基づいて判定される。

【0227】S2001で記録モードがデータ解析記録方式 (Cognizant Mode)、すなわち、Cognizant 記録の場合は、ステップS2002に進み、ディスク固有キー (Disc Unique Key) とタイトルキー (Title Key) と、データ解析記録方式用キー (Cognizant Key) とから、タイトル固有キー (Title Unique Key) を生成する。

【0228】S2001で記録モードがデータ非解析記

録方式 (Non-Cognizant Mode)、すなわち、Non-Cognizant 記録の場合は、ステップ S 2003 に進みディスク固有キー (Disc Unique Key) とタイトルキー (Title Key) と、データ非解析記録方式用キー (Non-Cognizant Key) とから、タイトル固有キー (Title Unique Key) を生成する。キー生成には、SHA-1 を用いる方法やブロック暗号に基づくハッシュ関数を使用する。

【0229】S1808では、記録再生装置は記録すべきコンテンツデータの被暗号化データをTSパケットの形で受信する。S1809で、TS処理手段300は、各TSパケットを受信した時刻情報であるATSを付加する。あるいはコピー制御情報CCIとATS、さらに他の情報を組み合わせた値を付加する。次に、S1810で、ATSを付加したTSパケットを順次受信し、1ブロックを形成する例えばX=32に達したか、あるいはパケットの終了を示す識別データを受信したかを判定する。いずれかの条件が満足された場合はステップS1811に進み、X個、あるいはパケット終了までのパケットを並べて、1ブロックのブロックデータを形成する。

【0230】次に、暗号処理手段150は、S1812で、ブロックデータの先頭の32ビット (ATSを含むブロック・シード) とS1807で生成したタイトル固有キーとから、そのブロックのデータを暗号化する鍵であるブロックキーを生成する。

【0231】S1813では、ブロックキーを用いてS1811で形成したブロックデータを暗号化する。なお、先にも説明したように、暗号化の対象となるのは、ブロックデータのm+1バイト目から最終データまでである。暗号化アルゴリズムは、たとえばIPS 46-2で規定されるDES (Data Encryption Standard) が適用される。

【0232】S1814で、暗号化したブロックデータを記録媒体に記録する。S1815で、全データを記録したかを判断する。全データを記録していれば、記録処理を終了し、全データを記録していなければS1808に戻って残りのデータの処理を実行する。

【0233】上述の処理にしたがって、コンテンツの記録処理がデータ解析記録方式 (Cognizant Mode) あるいは、データ非解析記録方式 (Non-Cognizant Mode) のいずれかによって実行される。コンテンツの記録処理がデータ解析記録方式 (Cognizant Mode) で実行される場合は、コンテンツの暗号化に適用される鍵が、データ解析記録方式用キー (Cognizant Key) に基づいて生成され、また、コンテンツの記録処理がデータ非解析記録方式 (Non-Cognizant Mode) で実行される場合は、コンテンツの暗号化に適用される鍵がデータ非解析記録方式用キー (Non-Cognizant Key) に基づいて生成されることになる。従って、それぞれの方式においてディスクに記録されたコンテンツは、記録時に使用したデータ解析記録方

式用キー (Cognizant Key)、あるいはデータ非解析記録方式用キー (Non-Cognizant Key) のいずれか、同一のキーを適用して復号用の鍵を生成することが必須となり、各方式が混在した記録、再生処理が防止される。

【0234】[秘密情報の書き込みおよび再生] 次に、図16、図17等にしたスタンプID等の秘密情報を、通常の方法で書き込み手法とは異なる態様でディスクに書き込み、また、通常の方法で読み出しとは異なる手法を適用した場合にのみ読み取り可能な態様とした秘密情報の書き込みおよび読み出し処理構成例について説明する。

【0235】(信号の擾乱による秘密情報生成) まず、スタンプID等の各種情報信号をM系列信号により擾乱して記録する構成について説明する。

【0236】図25に秘密情報の書き込み処理のための書き込み信号生成変調回路構成を示す。図25に示す変調回路は、データ書き込み対象であるディスク原盤が、所定の角度だけ回転する毎に信号レベルが立ち上がるFG信号を基準にしてスタンプID等の秘密情報の変調を行ない書き込みを実行する。

【0237】PLL回路1041は、FG信号を基準にディスク原盤の回転に同期したチャンネルクロックCKを生成して変調回路の各部に供給する。

【0238】タイミングジェネレータ1042は、チャンネルクロックCKをカウントすることにより、所定の時間間隔でM系列発生回路1045A~1045Dを初期化する初期化パルスSYを発生する。また、タイミングジェネレータ1042は、初期化パルスSYに同期した同期パターン選択信号STを生成して出力する。

【0239】図25に示す変調回路においては、チャンネルクロックCKに対して格段に遅いビットレートでスタンプID等の秘密情報が入力される。同期パターン発生回路1043は、初期化パルスSYの立ち上がりを基準にして所定の同期パターンDYを生成して出力する。

【0240】M系列発生回路1045a~1045Dは、初期化パルスSYにより初期化され、チャンネルクロックCK単位で変化するM系列M1~M4を出力する。ここでM系列M1~M4は、ランダムに論理値が変化する、かつ論理1と論理0との発生確率が等確立であるデータ列であり、相互に無相関である。

【0241】演算回路(X)1046A~1046Dは、エクスクルーシブオア回路により構成され、それぞれM系列信号M1~M4と、スタンプID、ディスクID等の秘密情報の各ビットb0~b3とエクスクルーシブオア演算を実行して演算結果を出力する。これにより、スタンプID等の秘密情報は、M系列信号M1~M4により擾乱される。

【0242】乱数発生回路1047は、2ビットの乱数(0, 1, 2, 3のいずれかの値)RをチャンネルクロックCK単位で発生し、データセクタ1048に出力す

る。データセクタ 1 0 4 8 は、乱数 R の値に応じて演算回路 1 0 4 6 A ~ 1 0 4 6 D の演算結果を選択出力する。例えば乱数 R = 0 のとき演算回路 1 0 4 6 A の出力選択、乱数 R = 1 のとき演算回路 1 0 4 6 B の出力選択、乱数 R = 2 のとき演算回路 1 0 4 6 C の出力選択、乱数 R = 3 のとき演算回路 1 0 4 6 D の出力選択とする。

【0 2 4 3】この構成により、変調回路は、対応する M 系列 M 1 ~ M 4 を基準にした復号により他の演算結果による影響を受けずに 1 0 4 6 A ~ 1 0 4 6 D の演算結果を 1 系統としてさらに擾乱する構成を可能としている。 10

【0 2 4 4】データセクタ 1 0 4 9 は、同期パターン信号 S T を基準にして同期パターン発生回路 1 0 4 3 から出力される同期パターン D Y、データセクタ 1 0 4 8 の出力を選択出力する。これにより、初期化パルス S Y が立ち上がった後、所定のクロック周期、例えば 5 クロック周期の間同期パターン [ e x . 1 1 0 1 1 ] の後、データセクタ 1 0 4 8 の出力を行なう。

【0 2 4 5】ディスク原盤には、所定の秘密情報書き込み領域に図 2 5 に示す変調回路において生成された出力が書き込まれる。変調回路に入力されるスタンパー I D 等の秘密情報が同一でも、乱数に応じて書き込みデータ 20 態様が異なることになる。従って通常の読み出し処理においては解析困難なデータの書き込みが可能となる。

【0 2 4 6】次に、上述の手法で書き込まれた秘密情報の再生処理について、図 2 6 を用いて説明する。図 2 6 は、ディスクから読み取られたデジタル再生信号 D X からスタンパー I D 等の秘密情報を復号する復号処理手段構成を示す図である。PLL 回路 1 0 8 1 は、ディスクから読み取られたデジタル再生信号 D X を基準にして記録時に生成したチャネルクロック C K を再生して各 30 部に出力する。

【0 2 4 7】同期検出回路 1 0 8 2 は、チャネルクロック C K を基準にしたデジタル再生信号 D X の識別により同期パターンを検出し、検出結果により記録時の初期化パルス S Y を再生する。M 系列発生回路 1 0 8 3 A ~ 1 0 8 3 D は、この初期化パルス S Y、チャネルクロック C K を基準にして、それぞれ記録時に生成した M 系列 M 1 ~ M 4 を出力する。

【0 2 4 8】乗算回路 ( X ) 1 0 8 4 A ~ 1 0 8 4 D は、それぞれ M 系列信号 M 1 ~ M 4 とデジタル再生信号 D X を乗算して乗算結果を出力する。なお、ここで乗算回路 ( X ) 1 0 8 4 A ~ 1 0 8 4 D は、M 系列信号 M 1 ~ M 4 の論理値に応じてデジタル再生信号 D X の極性を反転することにより、この乗算処理を実行する。デジタル再生信号 D X は、対応する M 系列 M 1 ~ M 4 を基準にした復号によってのみ正しく再生される。 40

【0 2 4 9】積分回路 1 0 8 5 A ~ 1 0 8 5 D は、乗算回路 1 0 8 4 A ~ 1 0 8 4 D により出力される乗算結果をそれぞれ初期化パルス S Y を基準にして積分することにより、スタンパー I D 等の秘密情報の対応するビット 50

列 b 1 ~ b 3 の論理値に応じた値の積分結果を出力する。判定回路 1 0 8 6 A ~ 1 0 8 6 D は、それぞれ積分回路 1 0 8 5 A ~ 1 0 8 5 D より出力される積分結果を初期化パルス S Y を基準にして 2 値識別することにより、スタンパー I D 等の秘密情報の各ビット b 0 ~ b 3 を復号して出力する。

【0 2 5 0】上述したように、スタンパー I D 等の秘密情報は、4 ビットパラレルビット列 b 0 ~ b 3 として変調回路 ( 図 2 5 ) に入力され、4 系統の M 系列 M 1 ~ M 4、また乱数 R による擾乱がなされて記録されるので、通常の読み出し処理での読み取りが困難となる。また、再生時には同期パターン D Y を基準にして M 系列 M 1 ~ M 4 を生成可能となり、生成した M 系列により、読み取り信号の復号により、スタンパー I D 等の秘密情報の出力が可能となる。

【0 2 5 1】上述の記録方式により書き込まれたスタンパー I D を読み取り、スタンパー I D 等に基づいてコンテンツの暗号処理鍵を生成する記録再生装置は、図 2 6 の構成を持つ秘密情報復号処理手段構成を持つ。

【0 2 5 2】( ディスク内周に秘密情報を記録 ) 次に、秘密情報の書き込み、再生処理の異なる例として、音楽データ等の書き込み領域とは異なるディスク領域にスタンパー I D 等の秘密情報を書き込み、これをフォーカスサーボにより安定的に読み取ることを可能とした構成について説明する。

【0 2 5 3】図 2 7 は、スタンパー I D 等の秘密情報を記録したディスクを示す斜視図である。スタンパー I D 等の秘密情報は、ディスクの 1 周に 4 回繰り返し記録され、部分的に損傷が発生した場合でも秘密情報の再生が可能となるように構成される。秘密情報は、ヘッダー、スタンパー I D 等の情報領域、さらに誤り訂正符号が割り当てられた構成を持つ。これらの情報を示すビットパターンの各ビットは、ユーザデータとして記録されるデータ領域の各ビットに比較して格段に長い、例えば 5 0 μ m 単位の微少領域を単位として形成される。また、スタンパー I D の情報領域、誤り訂正符号領域には、3 つの微少領域の中心領域のみ、記録面の光学特性を変化させたパターンが形成された同期パターンが形成され、この同期パターンにより、再生時のタイミング制御が可能となる。

【0 2 5 4】また、スタンパー I D 等の情報領域、誤り訂正符号領域データは、2 ビット毎にデータを区切り、2 ビットデータ ( b 1 , b 0 ) が、論理 0 0 の場合、図 2 7 ( D 1 ) に示すように、先頭の微少領域のみの記録面の光学特性を変化を発生させ、論理 [ 1 0 0 0 ] に変換して記録する。以下、( D 2 ) 2 ビットデータ ( b 1 , b 0 ) が、論理 0 1 の場合、[ 0 1 0 0 ]、( D 3 ) 2 ビットデータ ( b 1 , b 0 ) が、論理 1 0 の場合、[ 0 0 1 0 ]、( D 4 ) 2 ビットデータ ( b 1 , b 0 ) が、論理 1 1 の場合、[ 0 0 0 1 ] とする。これに

より、ディスク上には、光学特性の変化した領域の存在比率が0.3以下となり、ディスク内周領域においても十分な反射光量によるフォーカスサーボを可能としてデータ読み取りを可能となる。

【0255】図28は、ディスク内周領域に記録したスタンパーID等の秘密情報の読み取りに用いられる復号処理手段構成を示した図である。PLL回路1160は、デジタル再生信号DXよりチャネルクロックCKを再生出力する。

【0256】同期検出回路1161は、チャネルクロックCKを基準にしてデジタル再生信号DXの信号レベルを判定することにより、同期パターンを検出して初期化パルスSYを出力する。

【0257】タイミングジェネレータ1162は、初期化パルスSYを基準にして、同期パターンに続く図27に示す第1～4の微少領域について、それぞれ各微少領域のほぼ中央で立ち上がるサンプリングパルスT1～T4を出力する。

【0258】フリップフロップ（FF）1163A～1163Dは、それぞれサンプリングパルスT1～T4を基準にしてデジタル再生信号をラッチする。これにより、スタンパID、ディスクID等の情報領域、誤り訂正符号領域データの各2ビットに割り当てた4つの微少領域より得られる再生信号の信号レベルを、それぞれフリップフロップ1163A～1163Dにラッチして保持する。

【0259】最大値検出回路1164は、これら4つのラッチD1～D4の大小判定により、スタンパーID、ディスクID等の情報領域、誤り訂正符号領域の2ビットデータ（b1, b0）を復号して出力し、パラレルシリアル変換回路（PS）1165は、順次、最大値検出回路1164より出力される2ビットデータ（b1, b0）をシリアルデータに変換して出力する。

【0260】上述の記録方式により書き込まれたスタンパーIDを読み取り、スタンパーID等に基づいてコンテンツの暗号処理鍵を生成する記録再生装置は、図28の構成を秘密情報復号処理手段構成を持つ。

【0261】このように、コンテンツとは異なる特殊な秘密情報書き込み手法と読み取り手法の構成を採用して、スタンパーID等の秘密情報をディスクに格納し、これをコンテンツの暗号化、復号処理に適用する鍵の元データとして使用する構成としたので、たとえ他の処理キーが漏洩したとしても、ディスクに格納されたスタンパーID等の秘密情報は読み取りが困難であり、漏洩の可能性を激減させることが可能となり、よりセキュリティを高めたコンテンツ保護が可能となる。

【0262】なお、本明細書においては、ディスクに格納する特定のデータ書き込み処理、再生処理を要求される秘密情報をスタンパーIDとして設定した例を説明するが、スタンパーIDに限らず、ディスク毎に異なって

設定されるディスクID、コンテンツ毎に異なって設定するコンテンツID、あるいは暗号処理用のキー等、様々な識別データ、暗号処理鍵をディスクに格納する秘密情報として設定することが可能である。これらの様々な秘密情報を適用してコンテンツの暗号処理鍵を生成する。

【0263】なお、上述した記録再生装置は、図16、図17に示すように、データ解析記録方式（Cognizant Mode）記録用の暗号化、復号処理鍵生成用のキー（データ解析記録方式用キー（Cognizant Key））と、データ非解析記録方式（Non-Cognizant Mode）記録用の暗号化、復号処理鍵生成用のキー（データ非解析記録方式用キー（Non-Cognizant Key））との双方を選択的に使用可能な構成であるが、いずれか一方のみの方式を実行する記録再生機器においては、いずれか一方のキー、すなわちデータ解析記録方式用キー（Cognizant Key）、あるいはデータ非解析記録方式用キー（Non-Cognizant Key）のみを格納しており、格納キーに基づいてコンテンツの暗号化、復号処理用のブロックキーを生成する。これら単独のキーを格納した記録再生装置におけるコンテンツの暗号処理キーの生成処理過程を示すブロック図を図29、図30に示す。

【0264】図29は、データ解析記録方式用キー（Cognizant Key）のみを有する記録再生装置であり、記録媒体に対するデータ記録、記録媒体からのデータ再生の際に使用する暗号化キー、復号キーをデータ解析記録方式用キー（Cognizant Key）他のキー生成データに基づいて生成して、コンテンツの暗号化、復号を実行する構成である。

【0265】図30は、データ非解析記録方式用キー（Non-Cognizant Key）のみを有する記録再生装置であり、記録媒体に対するデータ記録、記録媒体からのデータ再生の際に使用する暗号化キー、復号キーをデータ非解析記録方式用キー（Non-Cognizant Key）他のキー生成データに基づいて生成して、コンテンツの暗号化、復号を実行する構成である。

【0266】これらの単独キー格納装置においては、いずれか一方の方式においてのみデータの記録、再生が実行可能となる。

【0267】〔世代管理のなされたマスターキーによるコンテンツデータ復号および再生処理〕次に、上記のようにして記録媒体に記録された暗号化コンテンツを復号して再生する処理について図31の処理ブロック図と、図32～図34のフローチャートを用いて説明する。

【0268】図31の処理ブロック図を参照しながら、図32に示すフローチャートに従って、復号処理および再生処理について、処理の流れを説明する。図32のS2401において、記録再生装置2300（図31参照）はディスク2320からディスクID2302とブレ（pre-recording）記録世代番号とスタンパーID（S

lamp ID) 2380を読み出し、また自身のメモリからマスターキー2301、データ解析記録方式用キー (Cognizant Key) 2331および/あるいはデータ非解析記録方式用キー (Non-Cognizant Key) 2332を読み出す。先の記録処理の説明から明らかなように、ディスクIDはディスクにあらかじめ記録されているか、そうでない場合は記録再生装置において生成してディスクに記録したディスク固有の識別子である。

【0269】プレ (pre-recording) 記録世代番号2360は、予め記録媒体であるディスクに格納されたディスク固有の世代情報である。このプレ (pre-recording) 世代番号と、データ記録時のマスターキーの世代番号、すなわち記録時世代番号2350を比較して再生処理の可否を制御する。マスターキー2301は、図14のフローにより記録再生装置のメモリに格納され世代管理のなされた秘密キーである。データ解析記録方式用キー (Cognizant Key) およびデータ非解析記録方式用キー (Non-Cognizant Key) は、それぞれデータ解析 (Cognizant) 記録モードおよびデータ非解析 (Non-Cognizant) 記録モードに対応したシステム共通の秘密キーである。

【0270】記録再生装置2300は、次に、S2402で、ディスクから読み出すべきデータのタイトルキー、さらに、データの記録モード、データを記録したときに使用したマスターキーの世代番号 (Generation #) すなわち記録時世代番号2350を読み出す。次に、S2403で読み出すべきデータが再生可能か否かを判定する。判定の詳細フローを図33に示す。

【0271】図33のステップS2501において、記録再生装置は、S2401で読み出したプレ世代番号と、S2402で読み出した記録時世代番号の新旧を判定する。記録時世代番号が示す世代が、プレ記録世代情報が表す世代以後でないと判定された場合、即ち、データ記録時世代情報が表す世代が、プレ記録世代情報が表す世代よりも古い世代である場合、再生不可能と判断し、ステップS2404乃至S2409をスキップして、再生処理を行わずに処理を終了する。従って、記録媒体に記録されたコンテンツが、プレ記録世代情報が表す世代よりも古い世代のマスターキーに基づいて暗号化されたものである場合には、その再生は許可されず、再生は行われない。

【0272】即ち、この処理は、不正が発覚して、最新の世代のマスターキーが与えられなくなった不正な記録装置で、古い世代のマスターキーに基づいて、データが暗号化され、記録媒体に記録された場合に該当するものと判断し、そのような不正な装置によってデータが記録された記録媒体の再生は行わないとした処理である。これにより、不正な記録装置の使用を排除することができる。

【0273】一方、ステップS2501において、記録時世代番号が表す世代が、プレ記録世代番号が表す世代

以後であると判定された場合、即ち、記録時世代情報が表す世代が、プレ記録世代番号が表す世代nと同一か、または新しい世代であり、従って、記録媒体に記録されたコンテンツが、プレ記録世代情報が表す世代以後の世代のマスターキーに基づいて暗号化されたものである場合には、ステップS2502に進み、記録再生装置は、自身のメモリが記憶している暗号化マスターキーCの世代情報を取得し、その暗号化マスターキーの世代と、暗号時世代情報が表す世代を比較して、その世代の前後を判定する。

【0274】ステップS2502において、メモリに記憶されたマスターキーCの世代が、記録時世代情報が表す世代以後でないと判定された場合、即ち、メモリに記憶されたマスターキーCの世代が、記録時世代情報が表す世代よりも古い世代である場合、再生不可能と判断し、ステップS2404乃至S2409をスキップして、再生処理を行わずに処理を終了する。

【0275】一方、ステップS2502において、メモリに記憶された暗号化マスターキーCの世代が、記録時世代情報が表す世代以後であると判定された場合、即ち、メモリに記憶されたマスターキーCの世代が、記録時世代情報が表す世代と同一か、またはそれよりも新しい場合、ステップS2503に進み、記録時のモードに対応する鍵、すなわちデータ解析記録方式用キー (Cognizant Key) もしくはデータ非解析記録方式用キー (Non-Cognizant Key) を、再生機器自身が所有しているかどうかを判断する。

【0276】ステップS2503において、記録時のモードに対応する鍵であるデータ解析記録方式用キー (Cognizant Key) もしくはデータ非解析記録方式用キー (Non-Cognizant Key) を、再生機器自身が所有している場合、再生可能と判定する。記録時のモードに対応する鍵 (データ解析記録方式用キー (Cognizant Key) もしくはデータ非解析記録方式用キー (Non-Cognizant Key)) を、再生機器自身が所有していない場合、再生不可能と判定する。

【0277】再生可能と判定された場合は、ステップS2404に進む。S2404では、ディスクID (Disc ID) とマスターキー (Master Key) とスタンパーID (Stamper ID) を用いてディスク固有キー (Disc Unique Key) を生成2302する。このキー生成方法は、例えば、FIPS 180-1で定められているハッシュ関数SHA-1に、マスターキーとディスクID (Disc ID) とのビット連結により生成されるデータを入力し、その160ビットの出力から必要なデータ長のみをディスク固有キー (Disc Unique Key) として使用する方や、ブロック暗号関数を用いたハッシュ関数にマスターキー (Master Key) とディスクID (Disc ID) を入力して得られた結果を用いるなどの方法が挙げられる。ここで使用するマスターキーは、図32のステップS2402で記録媒

体から読み出した、そのデータの記録時世代番号が表す世代（時点）のマスターキーである。もし記録再生装置がこれよりも新しい世代のマスターキーを保持している場合には、前述した方法を用いて記録時世代番号が表す世代のマスターキーを作成し、それを用いてディスク固有キー（Disc Unique Key）を生成してもよい。

【0278】次に、S2405で、タイトル固有キーの生成を行なう。タイトル固有キーの生成の詳細フローを図34に示す。暗号処理手段150は、ステップS2601において、記録モードの判定を実行する。この判定は、ディスクから読み出した記録モード（Recording Mode）に基づいて実行される。

【0279】S2601において、記録モードがデータ解析記録方式（Cognizant Mode）であると判定された場合は、ステップS2602に進み、ディスク固有キー（Disc Unique Key）とタイトルキー（Title Key）と、データ解析記録方式用キー（Cognizant Key）とから、タイトル固有キー（Title Unique Key）を生成する。

【0280】S2601において、記録モードがデータ非解析記録方式（Non-Cognizant Mode）であると判定された場合は、ステップS2603に進み、ディスク固有キー（Disc Unique Key）とタイトルキー（Title Key）と、データ非解析記録方式用キー（Non-Cognizant Key）とから、タイトル固有キー（Title Unique Key）を生成する。キー生成には、SHA-1を用いる方法やブロック暗号に基づくハッシュ関数を使用する。

【0281】なお、上記の説明では、マスターキー（Master Key）とスタンパーID（Stamper ID）とディスクID（Disc ID）からディスク固有キー（Disc Unique Key）を生成し、これとタイトルキー（Title Key）とデータ解析記録方式用キー（Cognizant Key）もしくはデータ非解析記録方式用キー（Non-Cognizant Key）からタイトル固有キー（Title Unique Key）をそれぞれ生成するようにしているが、ディスク固有キー（Disc Unique Key）を不要としてマスターキー（Master Key）とスタンパーID（Stamper ID）とディスクID（Disc ID）とタイトルキー（Title Key）と、データ解析記録方式用キー（Cognizant Key）もしくはデータ非解析記録方式用キー（Non-Cognizant Key）から直接タイトル固有キー（Title Unique Key）を生成してもよく、また、タイトルキー（Title Key）を用いずに、マスターキー（Master Key）とスタンパーID（Stamper ID）とディスクID（Disc ID）と、データ解析記録方式用キー（Cognizant Key）もしくはデータ非解析記録方式用キー（Non-Cognizant Key）からタイトル固有キー（Title Unique Key）相当の鍵を生成してもよい。

【0282】次にS2406でディスクから暗号化されて格納されている暗号化コンテンツ2312から順次ブロックデータ（Block Data）を読み出し、S2407で、ブロックデータの先頭の4バイトのブロック・シー

ド（Block Seed）をセクタ2310において分離して、ブロックシード（Block Seed）と、S2405で生成したタイトル固有キーを用いてブロックキーを生成する。

【0283】ブロック・キー（Block Key）の生成方法は、先に説明した図23の構成を適用することができる。すなわち、32ビットのブロック・シード（Block Seed）と、64ビットのタイトル固有キー（Title Unique Key）とから、64ビットのブロックキー（Block Key）を生成する構成が適用できる。

【0284】なお、上記説明ではディスク固有キー（Disc Unique key）、タイトル固有キー（Title Unique Key）、ブロックキー（Block Key）をそれぞれ生成する例を説明したが、たとえば、ディスク固有キー（Disc Unique Key）とタイトル固有キー（Title Unique Key）の生成を実行することなく、ブロックごとにマスターキー（Master Key）とスタンパーID（Stamper ID）とディスクID（Disc ID）とタイトルキー（Title Key）と、ブロックシード（Block Seed）と、データ解析記録方式用キー（Cognizant Key）もしくはデータ非解析記録方式用キー（Non-Cognizant Key）を用いてブロックキー（Block Key）を生成してもよい。

【0285】ブロックキーが生成されると、次にS2408で、ブロックキー（Block Key）を用いて暗号化されているブロックデータを復号2309し、セクタ2308を介して復号データとして出力する。なお、復号データには、トランスポートストリームを構成する各トランスポートパケットにATSが付加されており、先に説明したTS処理手段300において、ATSに基づくストリーム処理が実行される。その後、データは、使用、たとえば、画像を表示したり、音楽を再生したりすることが可能となる。

【0286】このように、ブロック単位で暗号化され記録媒体に格納された暗号化コンテンツはブロック単位でATSを含むブロック・シードに基づいて生成されるブロック鍵で復号処理が施されて再生が可能となる。ブロックキーを用いて暗号化されているブロックデータを復号し、S2409で、全データを読み出したかを判断し、全データを読み出していれば終了し、そうでなければS2406に戻り残りのデータを読み出す。

【0287】なお、上述した記録再生装置は、図31に示すように、データ解析記録方式（Cognizant Mode）記録用の暗号化、復号処理鍵生成用のキー（データ解析記録方式用キー（Cognizant Key））と、データ非解析記録方式（Non-Cognizant Mode）記録用の暗号化、復号処理鍵生成用のキー（データ非解析記録方式用キー（Non-Cognizant Key））との双方を選択的に使用可能な構成例であるが、先に図29、図30に示して説明したように、いずれか一方のキー、すなわちデータ解析記録方式用キー（Cognizant Key）、あるいはデータ非解析記録

方式用キー (Non-Cognizant Key) のみを格納した機器においては、いずれか一方のみの格納キーに対応する方式のみを実行し、格納キーに基づいてコンテンツの復号処理用のブロックキーを生成する。

【0288】〔記録媒体にのみ有効なメディアキーを使用した処理構成〕ところで、上記の実施例においては、有効化キーブロック (EKB: Enabling Key Block) を用いて各記録再生装置に対してマスターキーを伝送し、これを用いて記録再生装置がデータの記録、再生を行うとしていた。

【0289】マスターキーは、その時点におけるデータの記録全体に有効な鍵であり、ある時点のマスターキーを得ることができた記録再生装置は、その時点およびそれ以前にこのシステムで記録されたデータを復号することが可能になる。ただし、システム全体で有効であるというその性質上、マスターキーが攻撃者に露呈した場合の影響がシステム全体に及ぶという不具合もある。

【0290】これに対し、記録媒体のEKB (Enabling Key Block) を用いて伝送する鍵を、全システムに有効なマスターキーではなく、その記録媒体にのみ有効なメディアキーとすることにより、キーの露呈の影響を抑えることが可能となる。以下に、第2の実施例としてマスターキーの代わりにメディアキーを用いる方式を説明する。ただし、第1の実施例との変更部分のみを説明する。

【0291】図35には、図13と同様の例として、デバイス0が記録媒体に格納されている1時点のEKBと自分があらかじめ格納しているリーフキーK0000とノードキーK000、K00を用いて更新ノードキーK(t)00を生成し、これを用いて更新メディアキー: K(t) mediaを得る様子を示している。ここで得たK(t) mediaは、その記録媒体のデータの記録、再生時に使用される。

【0292】なお、図35におけるブレ記録世代番号 (Generation #n) は、メディアキーにおいてはマスターキーのように世代の新旧という概念はないので必須ではなくオプションとして設定される。

【0293】各記録再生装置は、たとえば、データの記録もしくは再生のために記録媒体が記録再生装置に挿入された際に、図36に示すフローチャートによってその記録媒体用のメディアキー: K(t) mediaを計算し、後にその記録媒体へのアクセスに使用する。

【0294】図36のステップS2801のEKBの読みこみとS2802のEKBの処理は、それぞれ図14のステップS1403およびS1404と同様の処理である。

【0295】ステップS2803において記録再生装置はメディアキーK(t) mediaをノードキー K(t) 00で暗号化した暗号文 Enc (K(t) 00, K(t) media) を記録媒体から読みこみ、ステップS2804で

これを復号してメディアキーを得る。もしこの記録再生装置が図11に示すツリー構成のグループから排除、すなわちリボークされていれば、メディアキーを入手できず、その記録媒体への記録および再生が行えない。

【0296】次に、記録媒体へのデータの記録の処理を説明するが、メディアキーにおいてはマスターキーのように世代の新旧という概念はないので、第1の実施例において図15に示した、ブレ記録世代情報と記録再生装置自身が格納するマスターキーの世代の比較による記録可能かどうかのチェックは行わず、上記処理においてメディアキーを得られていれば記録を行えると判断する。すなわち、図37に示す処理フローのようになる。図37の処理フローは、メディアキーの取得をS2901で判定し、取得された場合にのみ、ステップS2902においてコンテンツの記録処理を実行するものである。

【0297】〔記録媒体にのみ有効なメディアキーを使用したデータの記録処理〕コンテンツデータの記録処理の様子を、図38、39のブロック図および図40のフローチャートを用いて説明する。

【0298】本実施例では、第1の実施例と同様、記録媒体として光ディスクを例とする。この実施例では、記録媒体上のデータの bit-by-bit コピーを防ぐために、記録媒体固有の識別情報としてのディスクID (Disc ID) を、データを暗号化する鍵に作用させるようにしている点も同様である。

【0299】図38および図39は、それぞれ第1の実施例における図16および図17に対応する図であり、マスターキー (Master Key) の代わりにメディアキー (Media Key) が使われている点が異なっており、また、マスターキーの世代を示す記録時代番号 (Generation #) を用いていない点が異なっている。図38および図39の差異は、図16、図17の差異と同様ディスクIDの書き込みを実行するかしないかの差異である。

【0300】図40はメディアキーを用いる本実施例におけるデータ記録処理を示すものであり、前述した図18 (実施例1) のフローチャートに対応する。以下、図40の処理フローについて実施例1と異なる点を中心として説明する。

【0301】図40のS3201において、記録再生装置3000は自身のメモリに格納しているデータ解析記録方式用キー (Cognizant Key) および/もしくはデータ非解析記録方式用キー (Non-Cognizant Key) と、図36のS2804で計算し、一時的に保存しているメディアキーK(t) mediaを読み出す。また、ディスクからスタンパーID (Stamper ID) を読み出す。

【0302】S3202において、記録再生装置は記録媒体 (光ディスク) 3020に識別情報としてのディスクID (Disc ID) が既に記録されているかどうかを検査する。記録されていれば、S3203でこのディスクID (Disc ID) を読出し (図38に相当)、記録され

ていなければ、S3204で、ランダムに、もしくはあらかじめ定められた方法でディスクID (Disc ID) を生成し、ディスクに記録する(図39に相当)。ディスクID (Disc ID) はそのディスクにひとつあればよいので、リードインエリアなどに格納することも可能である。いずれの場合でも、次にS3205に進む。

【0303】S3205では、S3201で読み出したメディアキーとスタンパーID (Stamper ID) とディスクID (Disc ID) を用いて、ディスク固有キー (Disc Unique Key) を生成する。ディスク固有キー (Disc Unique Key) の具体的な生成方法としては、第1の実施例で使用した方法と同じ方法で、マスターキーの代わりにメディアキーを使用すればよい。

【0304】次にS3206に進み、その一回の記録ごとに固有の鍵: タイトルキー (Title Key) をランダムに、あるいはあらかじめ定められた方法で生成し、ディスクに記録する。同時に、このタイトル(データ)を記録したときの記録モード (Recording Mode) をディスクに記録する。

【0305】ディスク上には、どこかのデータがどんなタイトルを構成するかという情報が格納されたデータ管理ファイルがあり、このファイルにタイトルキー、Recording Mode を格納することができる。

【0306】ステップS3207乃至S3215は図18のS1807乃至S1815と同様であるため説明を省略する。

【0307】なお、上記の説明では、メディアキー (Media Key) とスタンパーID (Stamper ID) とディスクID (Disc ID) からディスク固有キー (Disc Unique Key) を生成し、これとタイトルキー (Title Key) とデータ解析記録方式用キー (Cognizant Key) もしくはデータ非解析記録方式用キー (Non-Cognizant Key) からタイトル固有キー (Title Unique Key) をそれぞれ生成するようにしているが、ディスク固有キー (Disc Unique Key) を不要としてメディアキー (Media Key) とスタンパーID (Stamper ID) とディスクID (Disc ID) とタイトルキー (Title Key) と、データ解析記録方式用キー (Cognizant Key) もしくはデータ非解析記録方式用キー (Non-Cognizant Key) から直接タイトル固有キー (Title Unique Key) を生成してもよく、また、タイトルキー (Title Key) を用いずに、メディアキー (Media Key) とスタンパーID (Stamper ID) とディスクID (Disc ID) と、データ解析記録方式用キー (Cognizant Key) もしくはデータ非解析記録方式用キー (Non-Cognizant Key) からタイトル固有キー (Title Unique Key) 相当の鍵を生成してもよい。

【0308】以上のようにして、メディアキーを用いて記録媒体にデータを記録することができる。

【0309】〔記録媒体にのみ有効なメディアキーを使用したデータの再生処理〕次に、上記のようにして記録

されたデータを再生する処理の様子を図41のブロック図と図42のフローチャートを用いて説明する。

【0310】図41は、第1の実施例における図31に対応する図であり、マスターキー (Master Key) の代わりにメディアキー (Media Key) が使われ、そのため記録時世代番号 (Generation #) が省略されている点が異なっている。

【0311】図42のS3401において、記録再生装置3400は記録媒体であるディスク3420からスタンパーID (Stamper ID) およびディスクID (Disc ID) を、また自身のメモリからデータ解析記録方式用キー (Cognizant Key) および/あるいはデータ非解析記録方式用キー (Non-Cognizant Key) と、図36のS2804で計算し一時的に保存しているメディアキーを読み出す。

【0312】なお、この記録媒体の挿入時に、図36の処理を行い、メディアキーを入手できなかった場合には、再生処理を行わずに終了する。

【0313】次にS3402で、ディスクから読み出すべきデータのタイトルキー (Title Key) とこのデータを記録した際の記録モード Recording Mode を読み出す。

【0314】次にS3403で、このデータが再生可能であるか否かを判断する。S3403の処理の詳細を図43に示す。

【0315】ステップS3501ではメディアキー (Media Key) を得られたか否かを判定する。メディアキーを得られなかった場合、再生不可能となり、メディアキーを得られた場合はステップS3502に進む。ステップS3502の処理は図33のS2503と同じであり、そのデータの記録時に使われた記録モードに対応する鍵 (データ解析記録方式 (Cognizant Mode) の場合、データ解析記録方式用キー (Cognizant Key)、データ非解析記録方式 (Non-Cognizant Mode) の場合、データ非解析記録方式用キー (Non-Cognizant Key)) を再生機器が持っている場合には「再生可能」と判断してステップS3404に進み、それ以外の場合には、「再生不可能」と判断して、ステップS3404乃至S3409をスキップして、再生処理を行わずに処理を終了する。

【0316】ステップS3404乃至S3409の処理は、図32のS2404乃至S2409と同様であるため、説明を省略する。

【0317】なお、上記の説明では、メディアキー (Media Key) とスタンパーID (Stamper ID) とディスクID (Disc ID) からディスク固有キー (Disc Unique Key) を生成し、これとタイトルキー (Title Key) と、データ解析記録方式用キー (Cognizant Key) もしくはデータ非解析記録方式用キー (Non-Cognizant Key) からタイトル固有キー (Title Unique Key) をそれぞれ生成するようにしているが、ディスク固有キー (Disc Unique Key) を不要としてメディアキー (Media Key) とスタンパ

ー ID (Stamper ID) とディスク ID (Disc ID) とタイトルキー (Title Key) と、データ解析記録方式用キー (Cognizant Key) もしくはデータ非解析記録方式用キー (Non-Cognizant Key) から直接タイトル固有キー (Title Unique Key) を生成してもよく、また、タイトルキー (Title Key) を用いずに、メディアキー (Media Key) とスタンパー ID (Stamper ID) とディスク ID (Disc ID) と、データ解析記録方式用キー (Cognizant Key) もしくはデータ非解析記録方式用キー (Non-Cognizant Key) からタイトル固有キー (Title Unique Key) 相当の鍵を生成してもよい。

【0318】上記のようにして、記録媒体へのデータの記録および記録媒体からの再生処理が実行される。

【0319】【記録処理におけるコピー制御】さて、コンテンツの著作権者等の利益を保護するには、ライセンスを受けた装置において、コンテンツのコピーを制御する必要がある。

【0320】即ち、コンテンツを記録媒体に記録する場合には、そのコンテンツが、コピーしても良いもの (コピー可能) かどうかを調査し、コピーして良いコンテンツだけを記録するようにする必要がある。また、記録媒体に記録されたコンテンツを再生して出力する場合には、その出力するコンテンツが、後で、違法コピーされないようにする必要がある。

【0321】そこで、そのようなコンテンツのコピー制御を行いながら、コンテンツの記録再生を行う場合の図 1 または図 2 の記録再生装置の処理について、図 4 4 および図 4 5 のフローチャートを参照して説明する。

【0322】まず、外部からのデジタル信号のコンテンツを、記録媒体に記録する場合においては、図 4 4 (A) のフローチャートにしたがった記録処理が行われる。図 4 4 (A) の処理について説明する。図 1 の記録再生器 100 を例として説明する。デジタル信号のコンテンツ (デジタルコンテンツ) が、例えば、IEEE1394 シリアルバス等を介して、入出力 I/F 120 に供給されると、ステップ S 4001 において、入出力 I/F 120 は、そのデジタルコンテンツを受信し、ステップ S 4002 に進む。

【0323】ステップ S 4002 では、入出力 I/F 120 は、受信したデジタルコンテンツが、コピー可能かどうかを判定する。即ち、例えば、入出力 I/F 120 が受信したコンテンツが暗号化されていない場合 (例えば、上述の D T C P を使用せずに、平文のコンテンツが、入出力 I/F 120 に供給された場合) には、そのコンテンツは、コピー可能であると判定される。

【0324】また、記録再生装置 100 が D T C P に準拠している装置であるとし、D T C P に従って処理を実行するものとする。D T C P では、コピーを制御するためのコピー制御情報としての 2 ビットの E M I (Encrypt

ion Mode Indicator) が規定されている。E M I が 00 B (B は、その前の値が 2 進数であることを表す) である場合は、コンテンツがコピーフリーのもの (Copy-free ly) であることを表し、E M I が 01 B である場合には、コンテンツが、それ以上のコピーをすることができないもの (No-more-copies) であることを表す。さらに、E M I が 10 B である場合は、コンテンツが、1 度だけコピーして良いもの (Copy-one-generation) であることを表し、E M I が 11 B である場合には、コンテンツが、コピーが禁止されているもの (Copy-never) であることを表す。

【0325】記録再生装置 100 の入出力 I/F 120 に供給される信号に E M I が含まれ、その E M I が、Copy-free ly や Copy-one-generation であるときには、コンテンツはコピー可能であると判定される。また、E M I が、No-more-copies や Copy-never であるときには、コンテンツはコピー可能でないと判定される。

【0326】ステップ S 4002 において、コンテンツがコピー可能でないと判定された場合、ステップ S 4003 ~ S 4005 をスキップして、記録処理を終了する。従って、この場合には、コンテンツは、記録媒体 10 に記録されない。

【0327】また、ステップ S 4002 において、コンテンツがコピー可能であると判定された場合、ステップ S 4003 に進み、以下、ステップ S 4003 ~ S 4005 において、図 3 (A) のステップ S 302、S 303、S 304 における処理と同様の処理が行われる。すなわち、T S 処理手段 300 によるトランスポートパケットに対する A T S 付加、暗号処理手段 150 における暗号化処理が実行され、その結果得られる暗号化コンテンツを、記録媒体 195 に記録して、記録処理を終了する。

【0328】なお、E M I は、入出力 I/F 120 に供給されるデジタル信号に含まれるものであり、デジタルコンテンツが記録される場合には、そのデジタルコンテンツとともに、E M I、あるいは、E M I と同様にコピー制御状態を表す情報 (例えば、D T C P における embedded CCI など) も記録される。

【0329】この際、一般的には、Copy-One-Generation を表す情報は、それ以上のコピーを許さないよう、No-more-copies に変換されて記録される。

【0330】本発明の記録再生装置では、この E M I や embedded CCI などのコピー制御情報を、T S パケットに付加する形で記録する。即ち、図 10 の例 2 や例 3 のように、A T S を 24 ビットないし 30 ビット分と、コピー制御情報を加えた 32 ビットを図 5 に示すように各 T S パケットに付加する。

【0331】外部からのアナログ信号のコンテンツを、記録媒体に記録する場合においては、図 4 4 (B) のフローチャートにしたがった記録処理が行われる。図 4 4

(B) の処理について説明する。アナログ信号のコンテンツ(アナログコンテンツ)が、入出力 I/F 140 に供給されると、入出力 I/F 140 は、ステップ S 4011 において、そのアナログコンテンツを受信し、ステップ S 4012 に進み、受信したアナログコンテンツが、コピー可能であるかどうかを判定する。

【0332】ここで、ステップ S 4012 の判定処理は、例えば、入出力 I/F 140 で受信した信号に、マクロビジョン(Macrovision)信号や、CGMS-A(Copy Generation Management System-Analog)信号が含まれるかどうかに基づいて行われる。即ち、マクロビジョン信号は、VHS 方式のビデオカセットテープに記録すると、ノイズとなるような信号であり、これが、入出力 I/F 140 で受信した信号に含まれる場合には、アナログコンテンツは、コピー可能でないと判定される。

【0333】また、例えば、CGMS-A 信号は、デジタル信号のコピー制御に用いられる CGMS 信号を、アナログ信号のコピー制御に適用した信号で、コンテンツがコピーフリーのもの(Copy-freely)、1 度だけコピーして良いもの(Copy-one-generation)、またはコピーが禁止されているもの(Copy-never)のうちのいずれであることを表す。

【0334】従って、CGMS-A 信号が、入出力 I/F 140 で受信した信号に含まれ、かつ、その CGMS-A 信号が、Copy-freely や Copy-one-generation を表している場合には、アナログコンテンツは、コピー可能であると判定される。また、CGMS-A 信号が、Copy-never を表している場合には、アナログコンテンツは、コピー可能でないと判定される。

【0335】さらに、例えば、マクロビジョン信号も、CGMS-A 信号も、入出力 I/F 4 で受信した信号に含まれない場合には、アナログコンテンツは、コピー可能であると判定される。

【0336】ステップ S 4012 において、アナログコンテンツがコピー可能でないと判定された場合、ステップ S 4013 乃至 S 4017 をスキップして、記録処理を終了する。従って、この場合には、コンテンツは、記録媒体 10 に記録されない。

【0337】また、ステップ S 4012 において、アナログコンテンツがコピー可能であると判定された場合、ステップ S 4013 に進み、以下、ステップ S 4013 乃至 S 4017 において、図 3 (B) のステップ S 322 乃至 S 326 における処理と同様の処理が行われ、これにより、コンテンツがデジタル変換、MPEG 符号化、TS 処理、暗号化処理がなされて記録媒体に記録され、記録処理を終了する。

【0338】なお、入出力 I/F 140 で受信したアナログ信号に、CGMS-A 信号が含まれている場合に、アナログコンテンツを記録媒体に記録するときには、その CGMS-A 信号も、記録媒体に記録される。即ち、

図 10 で示した CCI もしくはその他の情報の部分に、この信号が記録される。この際、一般的には、Copy-One-Generation を表す情報は、それ以上のコピーを許さないよう、No-more-copies に変換されて記録される。ただし、システムにおいてたとえば「Copy-one-generation のコピー制御情報は、No-more-copies に変換せずに記録するが、No-more-copies として扱う」などのルールが決められている場合は、この限りではない。

【0339】[再生処理におけるコピー制御] 次に、記録媒体に記録されたコンテンツを再生して、デジタルコンテンツとして外部に出力する場合においては、図 45 (A) のフローチャートにしたがった再生処理が行われる。図 45 (A) の処理について説明する。まず最初に、ステップ S 4101、S 4102、S 4103 において、図 4 (A) のステップ S 401、S 402、S 403 における処理と同様の処理が行われ、これにより、記録媒体から読み出された暗号化コンテンツが暗号処理手段 150 において復号処理がなされ、TS 処理がなされる。各処理が実行されたデジタルコンテンツは、バス 110 を介して、入出力 I/F 120 に供給される。

【0340】入出力 I/F 120 は、ステップ S 4104 において、そこに供給されるデジタルコンテンツが、後でコピー可能なものかどうかを判定する。即ち、例えば、入出力 I/F 120 に供給されるデジタルコンテンツに EMI、あるいは、EMI と同様にコピー制御状態を表す情報(コピー制御情報)が含まれない場合には、そのコンテンツは、後でコピー可能なものであると判定される。

【0341】また、例えば、入出力 I/F 120 に供給されるデジタルコンテンツに EMI 等のコピー制御情報が含まれる場合、従って、コンテンツの記録時に、DTC の規格にしたがって、EMI 等のコピー制御情報が記録された場合には、その EMI (記録された EMI (Recorded EMI)) 等のコピー制御情報が、Copy-freely であるときには、コンテンツは、後でコピー可能なものであると判定される。また、EMI 等のコピー制御情報が、No-more-copies であるときには、コンテンツは、後でコピー可能なものでないと判定される。

【0342】なお、一般的には、記録された EMI 等のコピー制御情報が、Copy-one-generation や Copy-never であることはない。Copy-one-generation の EMI は記録時に No-more-copies に変換され、また、Copy-never の EMI を持つデジタルコンテンツは、記録媒体に記録されないからである。ただし、システムにおいてたとえば「Copy-one-generation のコピー制御情報は、No-more-copies に変換せずに記録するが、No-more-copies として扱う」などのルールが決められている場合は、この限りではない。

【0343】ステップ S 4104 において、コンテンツが、後でコピー可能なものであると判定された場合、ス

ステップS4105に進み、入出力I/F120は、そのデジタルコンテンツを、外部に出力し、再生処理を終了する。

【0344】また、ステップS4104において、コンテンツが、後でコピー可能なものでないと判定された場合、ステップS4106に進み、入出力I/F120は、例えば、DTC Pの規格等にしがって、デジタルコンテンツを、そのデジタルコンテンツが後でコピーされないような形で外部に出力し、再生処理を終了する。

【0345】即ち、例えば、上述のように、記録されたEMI等のコピー制御情報が、No-more-copiesである場合（もしくは、システムにおいてたとえば「Copy-one-generationのコピー制御情報は、No-more-copiesに変換せずに記録するが、No-more-copiesとして扱う」というルールが決められていて、その条件下で記録されたEMI等のコピー制御情報がCopy-one-generationである場合）には、コンテンツは、それ以上のコピーは許されない。

【0346】このため、入出力I/F120は、DTC Pの規格にしたがい、相手の装置との間で認証を相互に行い、相手が正当な装置である場合（ここでは、DTC Pの規格に準拠した装置である場合）には、デジタルコンテンツを暗号化して、外部に出力する。

【0347】次に、記録媒体に記録されたコンテンツを再生して、アナログコンテンツとして外部に出力する場合においては、図45（B）のフローチャートにしたがった再生処理が行われる。図45（B）の処理について説明する。ステップS4111乃至S4115において、図4（B）のステップS421乃至S425における処理と同様の処理が行われる。すなわち、暗号化コンテンツの読み出し、復号処理、TS処理、MPEGデコード、D/A変換が実行される。これにより得られるアナログコンテンツは、入出力I/F140で受信される。

【0348】入出力I/F140は、ステップS4116において、そこに供給されるコンテンツが、後でコピー可能なものかどうかを判定する。即ち、例えば、記録されていたコンテンツにEMI等のコピー制御情報がいっしょに記録されていない場合には、そのコンテンツは、後でコピー可能なものであると判定される。

【0349】また、コンテンツの記録時に、たとえばDTC Pの規格にしたがって、EMI等のコピー制御情報が記録された場合には、その情報が、Copy-freelyであるときには、コンテンツは、後でコピー可能なものであると判定される。

【0350】また、EMI等のコピー制御情報が、No-more-copiesである場合、もしくは、システムにおいてたとえば「Copy-one-generationのコピー制御情報は、No-more-copiesに変換せずに記録するが、No-more-copies

として扱う」というルールが決められていて、その条件下で記録されたEMI等のコピー制御情報がCopy-one-generationである場合には、コンテンツは、後でコピー可能なものでないと判定される。

【0351】さらに、例えば、入出力I/F140に供給されるアナログコンテンツにCGMS-A信号が含まれる場合、従って、コンテンツの記録時に、そのコンテンツとともにCGMS-A信号が記録された場合には、そのCGMS-A信号が、Copy-freelyであるときには、アナログコンテンツは、後でコピー可能なものであると判定される。また、CGMS-A信号が、Copy-neverであるときには、アナログコンテンツは、後でコピー可能なものでないと判定される。

【0352】ステップS4116において、コンテンツが、後でコピー可能であると判定された場合、ステップS4117に進み、入出力I/F140は、そこに供給されたアナログ信号を、そのまま外部に出力し、再生処理を終了する。

【0353】また、ステップS4116において、コンテンツが、後でコピー可能でないと判定された場合、ステップS4118に進み、入出力I/F140は、アナログコンテンツを、そのアナログコンテンツが後でコピーされないような形で外部に出力し、再生処理を終了する。

【0354】即ち、例えば、上述のように、記録されたEMI等のコピー制御情報が、No-more-copiesである場合（もしくは、システムにおいてたとえば「Copy-one-generationのコピー制御情報は、No-more-copiesに変換せずに記録するが、No-more-copiesとして扱う」というルールが決められていて、その条件下で記録されたEMI等のコピー制御情報がCopy-one-generationである場合）には、コンテンツは、それ以上のコピーは許されない。

【0355】このため、入出力I/F140は、アナログコンテンツを、それに、例えば、マクロビジョン信号や、Copy-neverを表すCGMS-A信号を付加して、外部に出力する。また、例えば、記録されたCGMS-A信号が、Copy-neverである場合にも、コンテンツは、それ以上のコピーは許されない。このため、入出力I/F140は、CGMS-A信号をCopy-neverに変更して、アナログコンテンツとともに、外部に出力する。

【0356】以上のように、コンテンツのコピー制御を行いながら、コンテンツの記録再生を行うことにより、コンテンツに許された範囲外のコピー（違法コピー）が行われることを防止することが可能となる。

【0357】〔データ処理手段の構成〕なお、上述した一連の処理は、ハードウェアにより行うことは勿論、ソフトウェアにより行うこともできる。即ち、例えば、暗号処理手段150は暗号化／復号LSIとして構成することも可能であるが、汎用のコンピュータや、1チップ

のマイクロコンピュータにプログラムを実行させることにより行う構成とすることも可能である。同様にTS処理手段300も処理をソフトウェアによって実行することが可能である。一連の処理をソフトウェアによって行う場合には、そのソフトウェアを構成するプログラムが、汎用のコンピュータや1チップのマイクロコンピュータ等にインストールされる。図46は、上述した一連の処理を実行するプログラムがインストールされるコンピュータの一実施の形態の構成例を示している。

【0358】プログラムは、コンピュータに内蔵されている記録媒体としてのハードディスク4205やROM4203に予め記録しておくことができる。あるいは、プログラムはフロッピー（登録商標）ディスク、CD-ROM (Compact Disc Read Only Memory), MO (Magnetooptical) ディスク, DVD (Digital Versatile Disc), 磁気ディスク、半導体メモリなどのリムーバブル記録媒体4210に、一時的あるいは永続的に格納（記録）しておくことができる。このようなリムーバブル記録媒体4210は、いわゆるパッケージソフトウェアとして提供することができる。

【0359】なお、プログラムは、上述したようなリムーバブル記録媒体4210からコンピュータにインストールする他、ダウンロードサイトから、デジタル衛星放送用の人工衛星を介して、コンピュータに無線で転送したり、LAN (Local Area Network)、インターネットといったネットワークを介して、コンピュータに有線で転送し、コンピュータでは、そのようにして転送されてくるプログラムを、通信部4208で受信し、内蔵するハードディスク4205にインストールすることができる。

【0360】コンピュータは、CPU (Central Processing Unit) 4202を内蔵している。CPU 4202には、バス4201を介して、入出力インタフェース4211が接続されており、CPU 4202は、入出力インタフェース4210を介して、ユーザによって、キーボードやマウス等で構成される入力部4207が操作されることにより指令が入力されると、それにしたがって、ROM (Read Only Memory) 4203に格納されているプログラムを実行する。

【0361】あるいは、CPU 4202は、ハードディスク4205に格納されているプログラム、衛星若しくはネットワークから転送され、通信部4208で受信されてハードディスク4205にインストールされたプログラム、またはドライブ4209に装着されたリムーバブル記録媒体4210から読み出されてハードディスク4205にインストールされたプログラムを、RAM (Random Access Memory) 4204にロードして実行する。

【0362】これにより、CPU 4202は、上述したフローチャートにしたがった処理、あるいは上述したブロック図の構成により行われる処理を行う。そして、C

PU 4202は、その処理結果を、必要に応じて、例えば、入出力インタフェース4211を介して、LCD (Liquid Crystal Display) やスピーカ等で構成される出力部4206から出力、あるいは、通信部4208から送信、さらには、ハードディスク4205に記録させる。

【0363】ここで、本明細書において、コンピュータに各種の処理を行わせるためのプログラムを記述する処理ステップは、必ずしもフローチャートとして記載された順序に沿って時系列に処理する必要はなく、並列的あるいは個別に実行される処理（例えば、並列処理あるいはオブジェクトによる処理）も含むものである。

【0364】また、プログラムは、1のコンピュータにより処理されるものであっても良いし、複数のコンピュータによって分散処理されるものであっても良い。さらに、プログラムは、遠方のコンピュータに転送されて実行されるものであっても良い。

【0365】なお、本実施の形態では、コンテンツの暗号化／復号を行うブロックを、1チップの暗号化／復号LSIで構成する例を中心として説明したが、コンテンツの暗号化／復号を行うブロックは、例えば、図1および図2に示すCPU 170が実行する1つのソフトウェアモジュールとして実現することも可能である。同様に、TS処理手段300の処理もCPU 170が実行する1つのソフトウェアモジュールとして実現することが可能である。

【0366】〔記録媒体の製造装置および方法〕次に、上述した本発明の情報記録媒体を製造する本発明の情報記録媒体製造装置および方法について説明する。

【0367】図47には、記録媒体を製造すると共に、記録媒体に対してディスクID (Disk ID), 有効化キーブロック: EKB (Enabling Key Block) および、暗号化されたマスターキーまたは暗号化されたメディアキーを記録するディスク製造装置の概略構成を示す。

【0368】この図47に示すディスク製造装置は、図示しない組立工程により既に組み立てられている情報記録媒体に対して、ディスクID (Disk ID), 有効化キーブロック: EKB (Enabling Key Block) および、暗号化されたマスターキーまたは暗号化されたメディアキーを記録し、前述の秘密情報を記録する。さらに、必要に応じてマスターキーのプレ (pre-recording) 記録世代情報 (Generation#n) も併せて記録する。

【0369】ディスク製造装置4300は、ディスクID (Disk ID), 有効化キーブロック: EKB (Enabling Key Block) および、暗号化されたマスターキーまたは暗号化されたメディアキーをあらかじめ格納しているメモリ4302もしくはその他の記憶手段と、記録媒体4350に対する読み書きを行う記録媒体I/F 4303と、他の装置とのI/Fとなる入出力I/F 4304と、それらを制御する制御部4301、これらを接続するバス4305を備えている。

【0370】なお、図47の構成では、メモリ4302および記録媒体I/F4304は、当該製造装置に内蔵されている例を挙げているが、メモリ4302および記録媒体I/F4303は外付けのものであってもよい。

【0371】上記のディスクID (Disk ID) ,有効化キーブロック: EKB (Enabling KeyBlock) および、暗号化されたマスターキーまたは暗号化されたメディアキー、スタンパーID等の秘密情報、マスターキーのブレ (pre-recording) 記録世代情報 (Generation#n) は、たとえば図示しない識別子管理部門、鍵発行センター等により発行されるものであり、上記内蔵あるいは外付けのメモリにあらかじめ格納されている。

【0372】上記メモリ4302に格納されているディスクID (Disk ID) ,有効化キーブロック: EKB (Enabling Key Block) 、スタンパーID等の秘密情報および、暗号化されたマスターキーまたは暗号化されたメディアキーは、制御部4301の制御の下、記録媒体I/F4303を介して記録媒体に記録される。なお、必要に応じてマスターキーのブレ (pre-recording) 記録世代情報 (Generation#n) についても記録する。

【0373】なお、スタンパーID等の秘密情報は、前述の「秘密情報の書き込みおよび再生」欄で説明した例えば図25、図27等の構成を持つ秘密情報生成処理手段に従って生成されたデータであり、各構成に従って、スタンパーID等の秘密情報についてのデータ変換がなされ、その結果として得られる変換データが記録媒体に書き込まれる。

【0374】また、ディスクID (Disk ID) ,有効化キーブロック: EKB (Enabling KeyBlock) および、暗号化されたマスターキーまたは暗号化されたメディアキー、マスターキーのブレ (pre-recording) 記録世代情報 (Generation#n) は、上述したようにメモリ4302にあらかじめ格納されているものを使用するだけでなく、たとえば入出力I/F4304を介して鍵発行センタから送られてきたものを入手することも可能である。

【0375】図48には、本発明の記録媒体製造方法として、上記記録媒体を製造すると共に、記録媒体に対してディスクID (Disk ID) ,有効化キーブロック: EKB (Enabling Key Block) および、暗号化されたマスターキーまたは暗号化されたメディアキー、マスターキーのブレ (pre-recording) 記録世代情報 (Generation#n) を記録する記録媒体製造方法における製造工程の流れを示す。

【0376】図48において、記録媒体製造方法では、まず、ステップS4401の製造工程として、図示しない公知の組立工程によりDVD、CD等各種記録媒体が組み立てられる。

【0377】次に、ステップS4402の製造工程として、図47の記録媒体製造装置により、製造された記録媒体に対して、ディスクID (Disk ID) ,秘密情報とし

てのスタンパーID (Stamper ID) ,有効化キーブロック: EKB (Enabling Key Block) および、暗号化されたマスターキーまたは暗号化されたメディアキーの記録処理を実行する。また、必要に応じてマスターキーのブレ (pre-recording) 記録世代情報 (Generation#n) を記録する。

【0378】以上のディスク製造処理プロセスにより、記録媒体は、ディスクID (Disk ID) ,有効化キーブロック: EKB (Enabling Key Block) および、暗号化されたマスターキーまたは暗号化されたメディアキー、および秘密情報としてのスタンパーIDを記録した状態で製造工場から出荷される。また、必要に応じてマスターキーのブレ (pre-recording) 記録世代情報 (Generation#n) を記録した後、製造工場から出荷される。

【0379】なお、秘密情報として記録するのはスタンパーIDに限らず、ディスク毎に異なって設定されるディスクID、コンテンツ毎に異なって設定するコンテンツID、あるいは暗号処理用のキー等、様々な識別データ、暗号処理鍵をディスクに格納する秘密情報として記録してもよい。記録再生装置においては、これらの様々な秘密情報を適用してコンテンツの暗号処理鍵を生成する。

【0380】[EKBのフォーマット] 図49に有効化キーブロック (EKB: Enabling Key Block) のフォーマット例を示す。バージョン4501は、有効化キーブロック (EKB: Enabling KeyBlock) のバージョンを示す識別子である。デブス4502は、有効化キーブロック (EKB: Enabling Key Block) の配布先のデバイスに対する階層ツリーの階層数を示す。データポインタ4503は、有効化キーブロック (EKB: Enabling Key Block) 中のデータ部の位置を示すポインタであり、タグポインタ4504はタグ部の位置、署名ポインタ4505は署名の位置を示すポインタである。データ部4506は、例えば更新するノードキーを暗号化したデータを格納する。

【0381】タグ部4507は、データ部に格納された暗号化されたノードキー、リーフキーの位置関係を示すタグである。このタグの付与ルールを図50を用いて説明する。図50では、データとして先に図12 (A) で説明した有効化キーブロック (EKB) を送付する例を示している。この時のデータは、図50の右の表に示ようになる。このときの暗号化キーに含まれるトップノードのアドレスをトップノードアドレスとする。この場合は、ルートキーの更新キーK (t) Rが含まれているので、トップノードアドレスはKRとなる。

【0382】暗号化キーの最上段のデータEnc (K (t) 0, K (t) R) は、図50の左の階層ツリーに示す位置にある。ここで、次のデータは、Enc (K (t) 0 0, K (t) 0) であり、ツリー上では前のデータの左下の位置にある。データがある場合は、タグが

10

20

30

40

50

0、ない場合は1が設定される。タグは{左(L)タグ、右(R)タグ}として設定される。最上段のデータ Enc (K (t) 0, K (t) R) の左にはデータがあるので、Lタグ=0、右にはデータがないので、Rタグ=1となる。以下、すべてのデータにタグが設定され、図50(c)に示すデータ列、およびタグ列が構成される。

【0383】ツリーのノード処理の順番として、同一段の幅方向を先に処理する幅優先(breadth first)処理と、深さ方向を先に処理する深さ優先(depth first)処理のいずれかをを用いるのが好適である。

【0384】図49に戻って、EKBフォーマットについてさらに説明する。署名(Signature)は、有効化キープブロック(EKB)を発行した例えば鍵管理センタ、コンテンツロバイダ、決済機関等が実行する電子署名である。EKBを受領したデバイスは署名検証によって正当な有効化キープブロック(EKB)発行者が発行した有効化キープブロック(EKB)であることを確認する。

【0385】以上、特定の実施例を参照しながら、本発明について詳解してきた。しかしながら、本発明の要旨を逸脱しない範囲で当業者が該実施例の修正や代用を成し得ることは自明である。例えば、前述したように、実施例においては、ディスクに格納する特定のデータ書き込み処理、再生処理を要求される秘密情報をスタンパーIDとした例を説明したが、スタンパーIDに限らず、ディスク毎に異なって設定されるディスクID、コンテンツ毎に異なって設定するコンテンツID、あるいは暗号処理用のキー等、様々な識別データ、暗号処理鍵をディスクに格納する秘密情報として設定することが可能である。実施例においては、例示という形態で本発明を開示してきたのであり、限定的に解釈されるべきではない。本発明の要旨を判断するためには、冒頭に記載した特許請求の範囲の欄を参酌すべきである。

【0386】

【発明の効果】上述したように、本発明の構成においては、記録媒体に、あらかじめその書き込み/読出し方法が解析困難な、特殊の読み出し方法でのみ読み取り可能な秘密情報の信号を格納し、この記録媒体に対する音楽データ、画像データ等のコンテンツの記録あるいは再生を行う際のコンテンツ暗号化あるいは復号処理用暗号鍵に、上記の秘密情報を作用させる構成とした。従って、特定の読み取り方法を実行可能な正当デバイスにおいてのみ、秘密情報の読み取り、コンテンツの暗号処理鍵の生成が可能となり、秘密情報の読み取り方法の実行できないデバイスにおけるコンテンツ再生を効果的に防止することが可能となる。

【0387】また、本発明の構成においては、特殊の読み出し方法でのみ読み取り可能な秘密情報は、正当なデバイス、すなわち秘密情報の読み取り方法を実行可能なデバイスでのみ読み取られ、たとえばLSI内に実装さ

れて高度に保護された暗号鍵の生成を実行する暗号処理部においてセキュアな保護の下にコンテンツ暗号処理用の鍵生成処理に使用される構成であり、秘密情報が外部からの読み取り可能なメモリ上に格納されない。従って、秘密情報の漏洩の可能性がなく、不正なコンテンツの再生処理を効果的に防止することが可能となる。

【0388】また、本発明の構成によれば、ツリー

(木)構造の鍵配布構成により、マスターキーやメディアキーの更新データを有効化キープブロック(EKB)とともに送信し、送信したマスターキーやメディアキーと、特殊な読み取り手法でのみ読み取り可能な秘密情報とに基づいてコンテンツ暗号化あるいは復号処理用暗号鍵生成処理を実行する構成としたので、秘密情報についての特殊な読み取り方法を実行可能で、かつツリー構造の鍵配布構成により鍵の配布された正当デバイスでのみコンテンツの利用が可能となる。

【図面の簡単な説明】

【図1】本発明の情報記録再生装置の構成例(その1)を示すブロック図である。

【図2】本発明の情報記録再生装置の構成例(その2)を示すブロック図である。

【図3】本発明の情報記録再生装置のデータ記録処理フローを示す図である。

【図4】本発明の情報記録再生装置のデータ再生処理フローを示す図である。

【図5】本発明の情報記録再生装置において処理されるデータフォーマットを説明する図である。

【図6】本発明の情報記録再生装置におけるトランスポート・ストリーム(TS)処理手段の構成を示すブロック図である。

【図7】本発明の情報記録再生装置において処理されるトランスポート・ストリームの構成を説明する図である。

【図8】本発明の情報記録再生装置におけるトランスポート・ストリーム(TS)処理手段の構成を示すブロック図である。

【図9】本発明の情報記録再生装置におけるトランスポート・ストリーム(TS)処理手段の構成を示すブロック図である。

【図10】本発明の情報記録再生装置において処理されるブロックデータの付加情報としてのブロック・データの構成例を示す図である。

【図11】本発明の情報記録再生装置に対するマスターキー、メディアキー等の鍵の暗号化処理について説明するツリー構成図である。

【図12】本発明の情報記録再生装置に対するマスターキー、メディアキー等の鍵の配布に使用される有効化キープブロック(EKB)の例を示す図である。

【図13】本発明の情報記録再生装置におけるマスターキーの有効化キープブロック(EKB)を使用した配布例

ど復号処理例を示す図である。

【図 1 4】本発明の情報記録再生装置におけるマスターキーの有効化キーブロック (EKB) を使用した復号処理フローを示す図である。

【図 1 5】本発明の情報記録再生装置におけるコンテンツ記録処理におけるマスターキーの世代比較処理フローを示す図である。

【図 1 6】本発明の情報記録再生装置において、データ記録処理時の暗号化処理を説明するブロック図 (その 1) である。

【図 1 7】本発明の情報記録再生装置において、データ記録処理時の暗号化処理を説明するブロック図 (その 2) である。

【図 1 8】本発明の情報記録再生装置において、データ記録処理を説明するフローチャートである。

【図 1 9】本発明の情報記録再生装置におけるディスク固有キーの生成例を説明する図である。

【図 2 0】本発明の情報記録再生装置において処理される伝送 1394 パケットにおける EMI 格納位置 (5CDTCP 規格) を示す図である。

【図 2 1】本発明の情報記録再生装置におけるコンテンツ記録をデータ解析記録方式 (Cognizant Mode) によって実行するか、データ非解析記録方式 (Non-Cognizant Mode) で実行するかを決定するプロセスを説明するフロー図である。

【図 2 2】本発明の情報記録再生装置において、データ記録時のタイトル固有キーの生成処理例を示す図である。

【図 2 3】本発明の情報記録再生装置におけるブロック・キーの生成方法を説明する図である。

【図 2 4】本発明の情報記録再生装置におけるタイトル固有キーの生成処理フローを示す図である。

【図 2 5】本発明の情報記録再生装置におけるスタンパー ID 等の秘密情報の記録処理に適用される変調回路を示す図である。

【図 2 6】図 2 5 に示すスタンパー ID 等の秘密情報の再生処理に適用される秘密情報復号処理回路を示す図である。

【図 2 7】本発明の情報記録再生装置におけるスタンパー ID 等の秘密情報の記録構成例を示す図である。

【図 2 8】図 2 7 に示すスタンパー ID 等の秘密情報の再生処理に適用される秘密情報復号処理回路を示す図である。

【図 2 9】本発明の情報記録再生装置におけるデータ解析記録用キーのみを格納した記録再生装置構成例を示す図である。

【図 3 0】本発明の情報記録再生装置におけるデータ非解析記録用キーのみを格納した記録再生装置構成例を示す図である。

【図 3 1】本発明の情報記録再生装置において、データ

再生処理時のコンテンツデータ復号処理を説明するブロック図である。

【図 3 2】本発明の情報記録再生装置において、データ再生処理を説明するフローチャートである。

【図 3 3】本発明の情報記録再生装置において、データ再生処理における再生可能制判定処理の詳細を示すフローチャートである。

【図 3 4】本発明の情報記録再生装置において、データ再生時のタイトル固有キーの生成処理フローを示す図である。

【図 3 5】本発明の情報記録再生装置におけるメディアキーの有効化キーブロック (EKB) を使用した配布例と復号処理例を示す図である。

【図 3 6】本発明の情報記録再生装置におけるメディアキーの有効化キーブロック (EKB) を使用した復号処理フローを示す図である。

【図 3 7】本発明の情報記録再生装置におけるメディアキーを使用したコンテンツ記録処理フローを示す図である。

【図 3 8】本発明の情報記録再生装置において、メディアキーを使用したデータ記録処理時の暗号化処理を説明するブロック図 (その 1) である。

【図 3 9】本発明の情報記録再生装置において、メディアキーを使用したデータ記録処理時の暗号化処理を説明するブロック図 (その 2) である。

【図 4 0】本発明の情報記録再生装置において、メディアキーを使用したデータ記録処理を説明するフローチャートである。

【図 4 1】本発明の情報記録再生装置において、メディアキーを使用したデータ再生処理時の暗号化処理を説明するブロック図である。

【図 4 2】本発明の情報記録再生装置において、メディアキーを使用したデータ再生処理を説明するフローチャートである。

【図 4 3】本発明の情報記録再生装置において、メディアキーを使用したデータ再生処理における再生可能性判定処理の詳細を示すフローチャートである。

【図 4 4】本発明の情報記録再生装置におけるデータ記録処理時のコピー制御処理を説明するフローチャートである。

【図 4 5】本発明の情報記録再生装置におけるデータ再生処理時のコピー制御処理を説明するフローチャートである。

【図 4 6】本発明の情報記録再生装置において、データ処理をソフトウェアによって実行する場合の処理手段構成を示したブロック図である。

【図 4 7】本発明の情報記録再生装置において使用される情報記録媒体を製造する製造装置の構成を示すブロック図である。

【図 4 8】本発明の情報記録再生装置において使用され

る情報記録媒体を製造する製造処理の処理フローを示す図である。

【図 49】本発明の情報記録再生装置において使用される有効化キーブロック (EKB) のフォーマット例を示す図である。

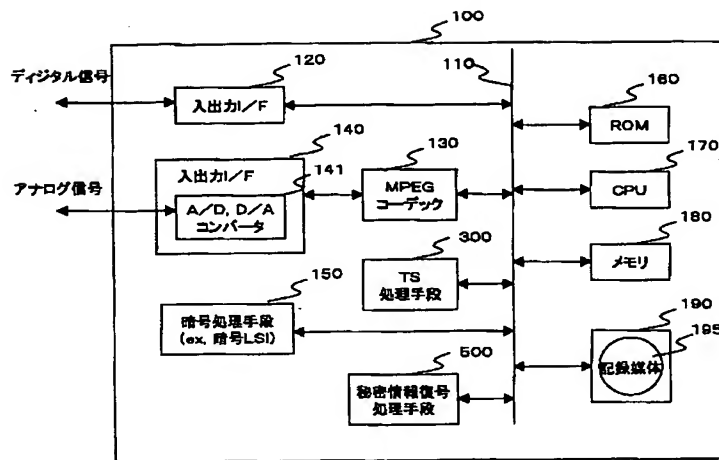
【図 50】本発明の情報記録再生装置において使用される有効化キーブロック (EKB) のタグの構成を説明する図である。

【符号の説明】

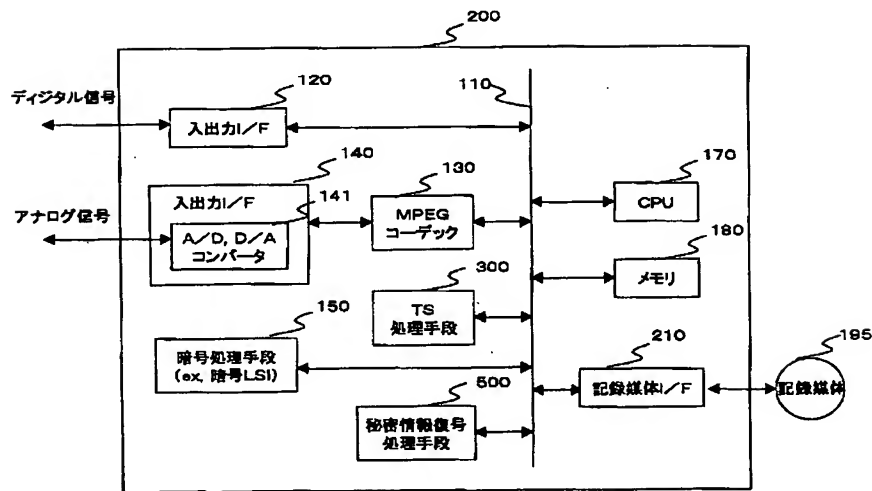
100, 200 記録再生装置  
 110 バス  
 120 入出力 I/F  
 130 MPEGコーデック  
 140 入出力 I/F  
 141 A/D, D/Aコンバータ  
 150 暗号処理手段  
 160 ROM  
 170 CPU  
 180 メモリ  
 190 ドライブ  
 195 記録媒体  
 210 記録媒体 I/F  
 300 TS処理手段  
 500 秘密情報復号処理手段  
 600, 607 端子  
 602 ビットストリームパーサ  
 603 PLL  
 604 タイムスタンプ発生回路  
 605 ブロックシード付加回路  
 606 スムージングバッファ  
 800, 806 端子  
 801 ブロックシード分離回路  
 802 出力制御回路  
 803 比較器  
 804 タイミング発生回路  
 805 27MHzクロック  
 901, 904, 913 端子  
 902 MPEGビデオエンコーダ  
 903 ビデオストリームバッファ  
 905 MPEGオーディオエンコーダ  
 906 オーディオストリームバッファ  
 908 多重化スケジューラ  
 909 トランスポートバケット符号化器  
 910 到着タイムスタンプ計算手段  
 911 ブロックシード付加回路  
 912 スムージングバッファ

976 スイッチ  
 1041 PLL回路  
 1042 タイミングジェネレータ  
 1043 同期パターン発生回路  
 1045 M系列発生回路  
 1046 演算回路  
 1047 乱数発生回路  
 1048 データセレクト  
 1049 データセレクト  
 1081 PLL回路  
 1082 同期検出回路  
 1083 M系列発生回路  
 1084 乗算回路  
 1085 積分回路  
 1086 判定回路  
 1160 PLL回路  
 1161 同期検出回路  
 1162 タイミングジェネレータ  
 1163 フリップフロップ  
 1164 最大値検出回路  
 1165 パラレルシリアル変換回路  
 4202 CPU  
 4203 ROM  
 4204 RAM  
 4205 ハードディスク  
 4206 出力部  
 4207 入力部  
 4208 通信部  
 4209 ドライブ  
 4210 リムーバブル記録媒体  
 4211 入出力インタフェース  
 4300 ディスク製造装置  
 4301 制御部  
 4302 メモリ  
 4303 記録媒体 I/F  
 4304 入出力 I/F  
 4305 バス  
 4350 記録媒体  
 4501 バージョン  
 4502 デブス  
 4503 データポインタ  
 4504 タグポインタ  
 4505 署名ポインタ  
 4506 データ部  
 4507 タグ部  
 4508 署名

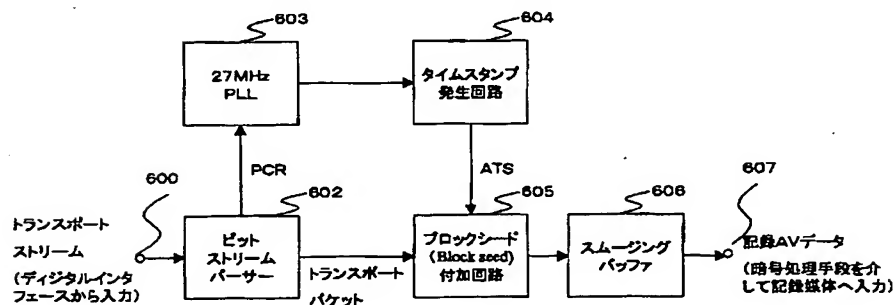
【図1】



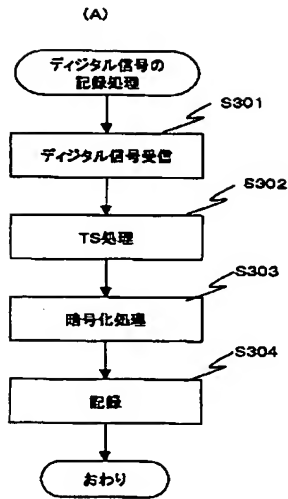
【図2】



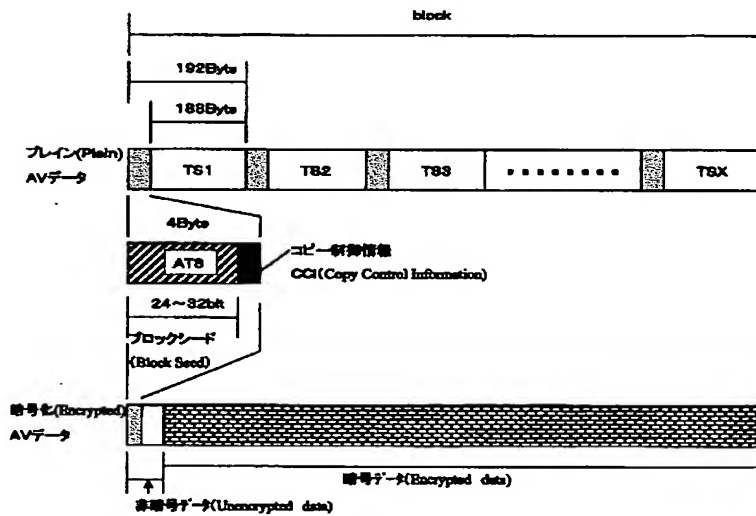
【図6】



【図 3】



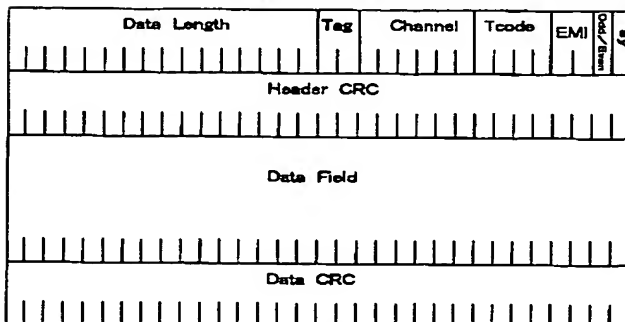
【図 5】



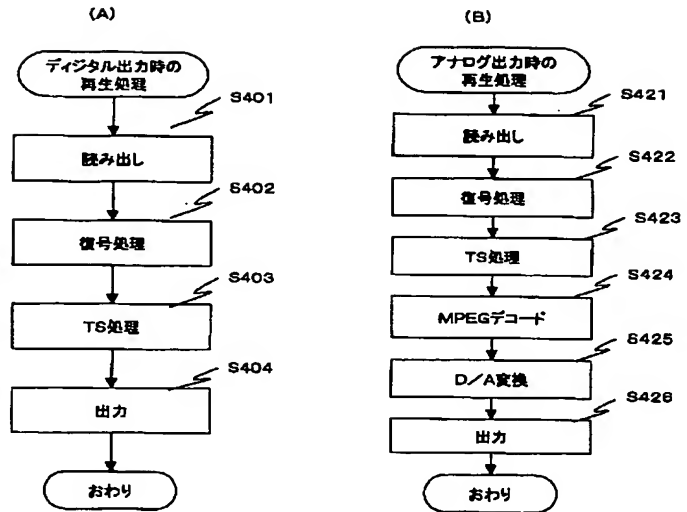
【図 20】

Transmitted First

313029262728252423222120191817161514131211109 8 7 6 5 4 3 2 1 0



【図 4】



【図 12】

(A) キー更新ブロック(KRB: Key Renewal Block) 例1

デバイス0, 1, 2にt時点でのルートキー-K(t)Rを送付

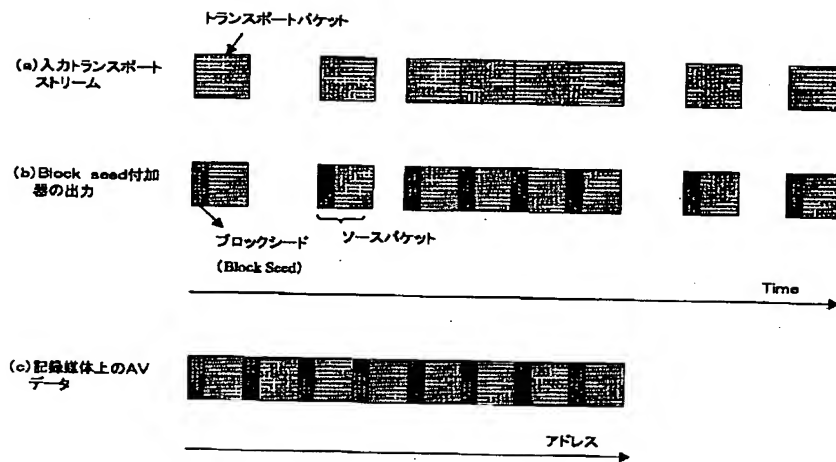
世代(Generation): t	
インデックス	暗号化キー
0	Enc(K(t)0, K(t)R)
00	Enc(K(t)00, K(t)0)
000	Enc(K000, K(t)00)
001	Enc(K(t)001, K(t)00)
0010	Enc(K0010, K(t)001)

(B) キー更新ブロック(KRB: Key Renewal Block) 例2

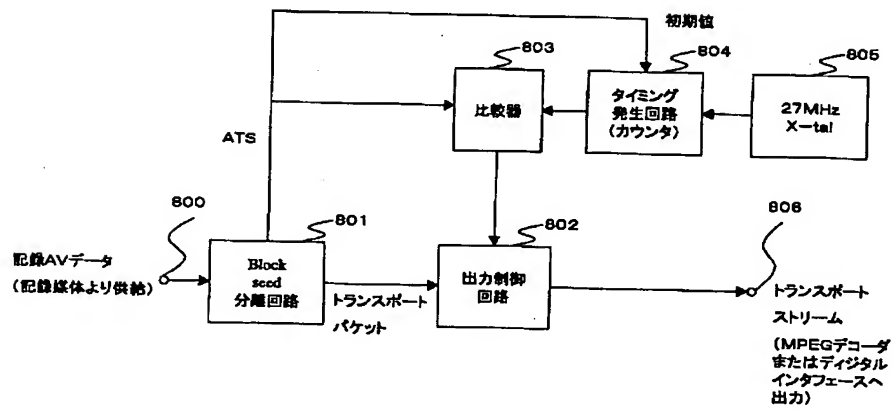
デバイス0, 1, 2にt時点でのルートキー-K(t)Rを送付

世代(Generation): t	
インデックス	暗号化キー
000	Enc(K000, K(t)00)
001	Enc(K(t)001, K(t)00)
0010	Enc(K0010, K(t)001)

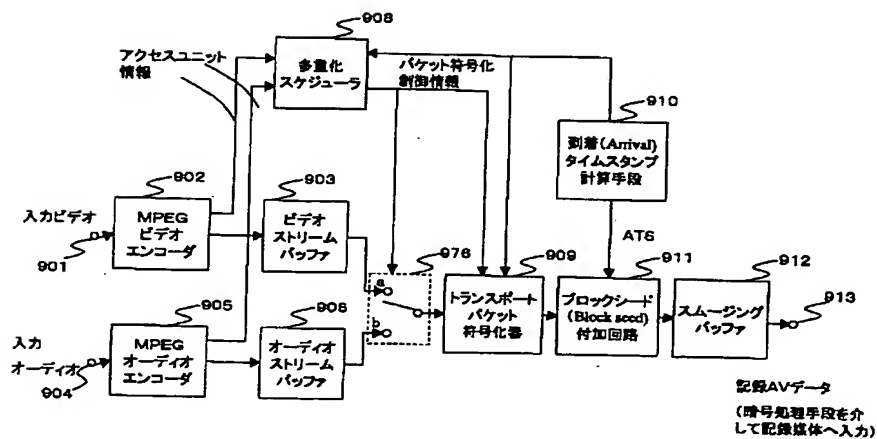
【図 7】



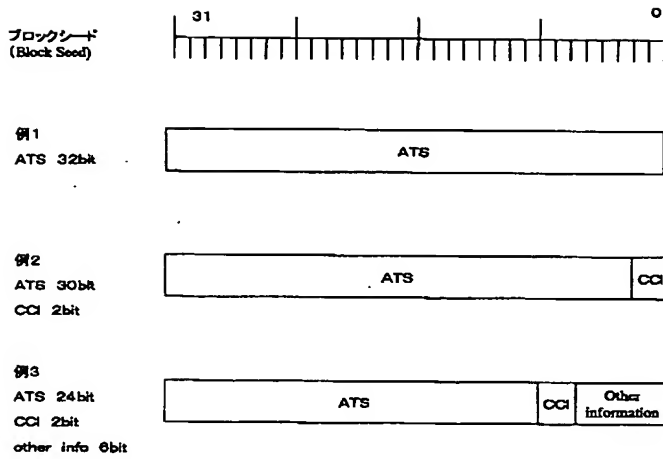
【図 8】



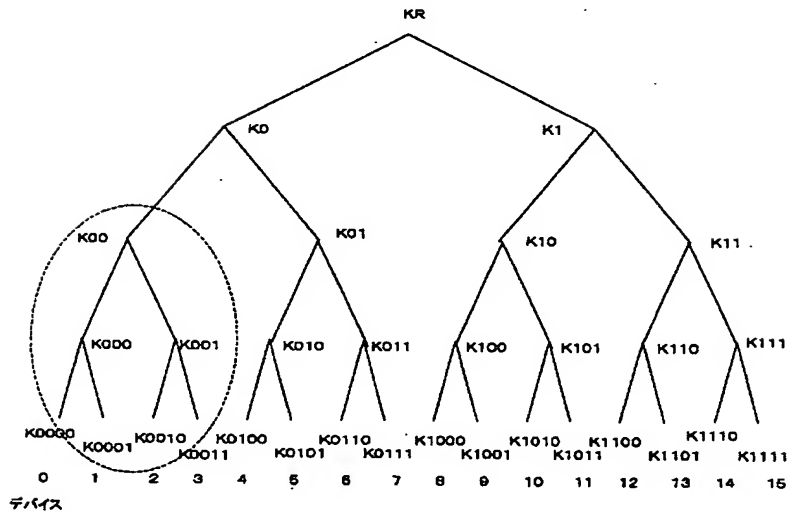
【図 9】



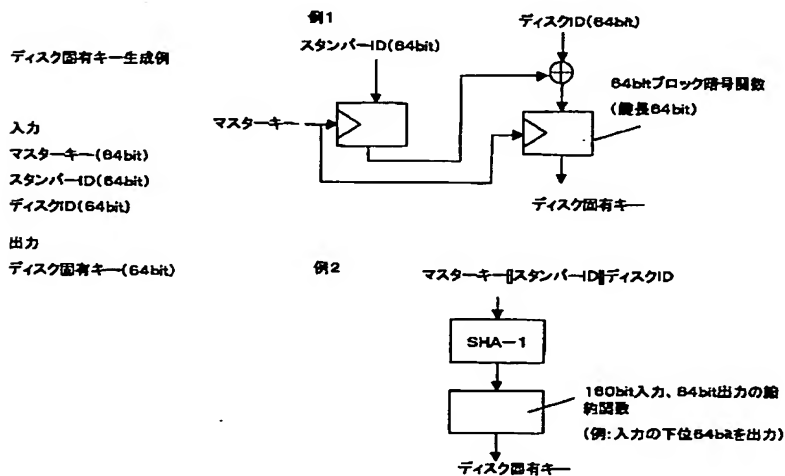
【図 10】



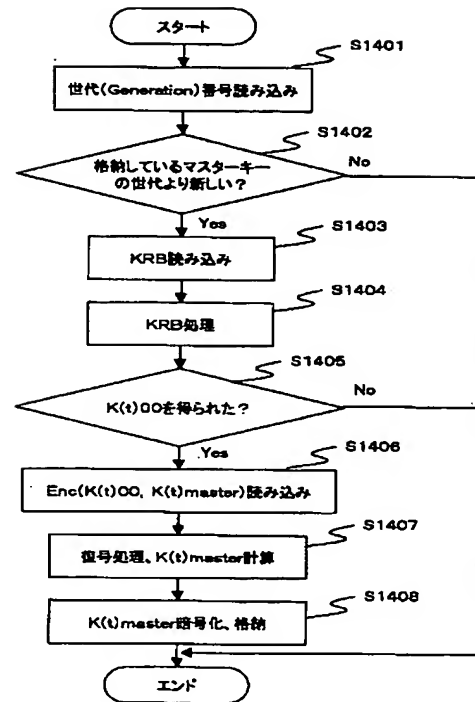
【図 11】



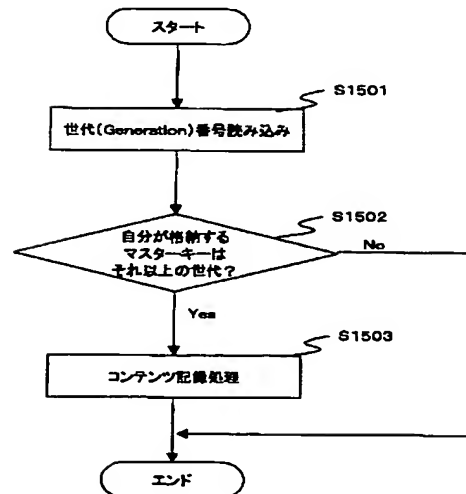
【図 19】



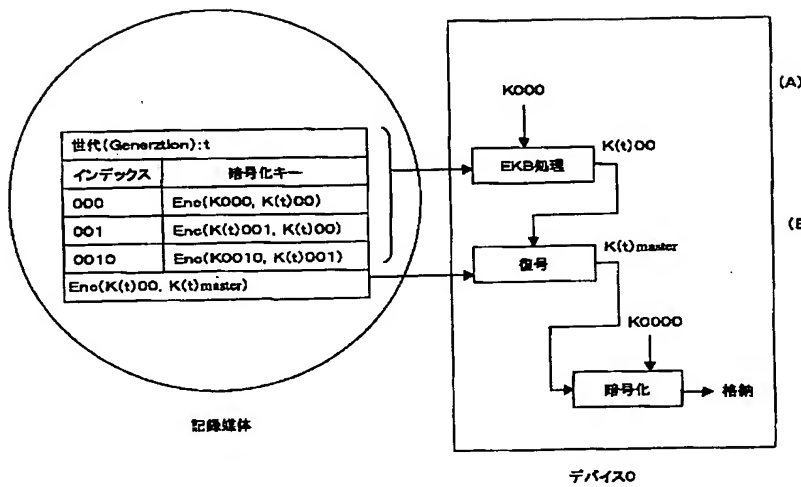
【図 14】



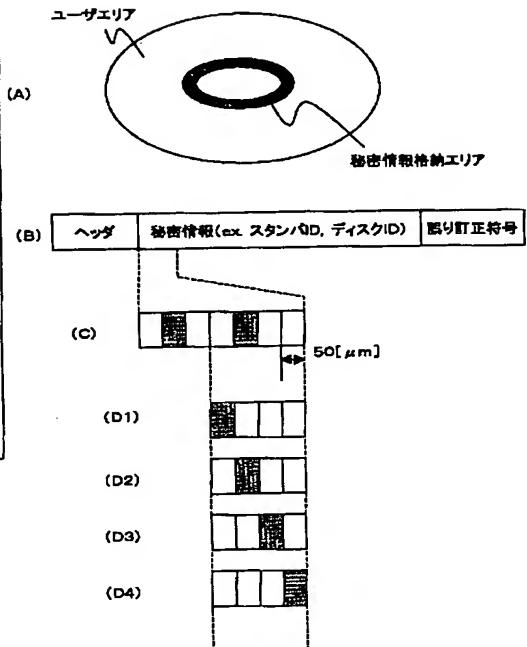
【図 15】



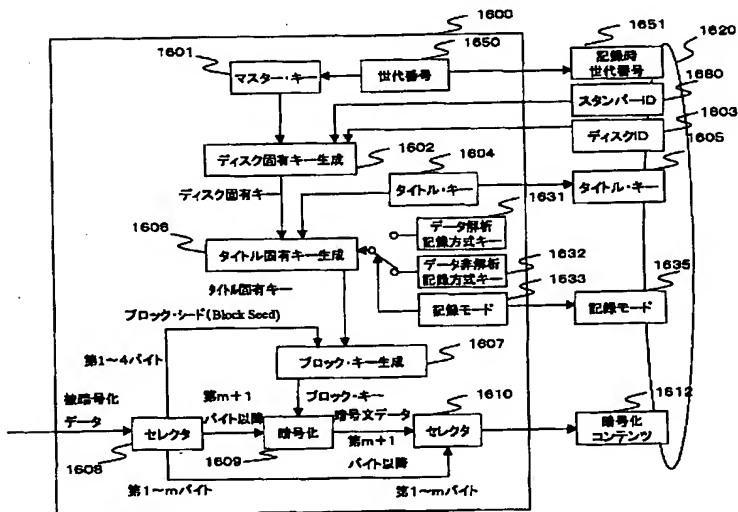
【図 13】



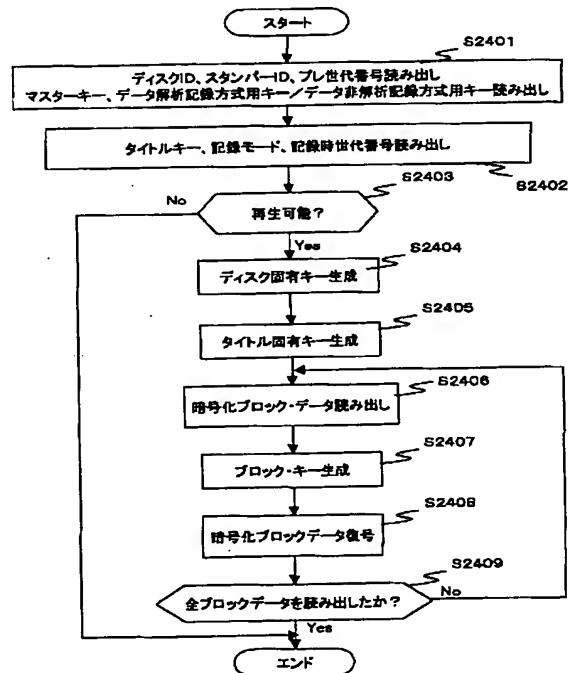
【図 27】



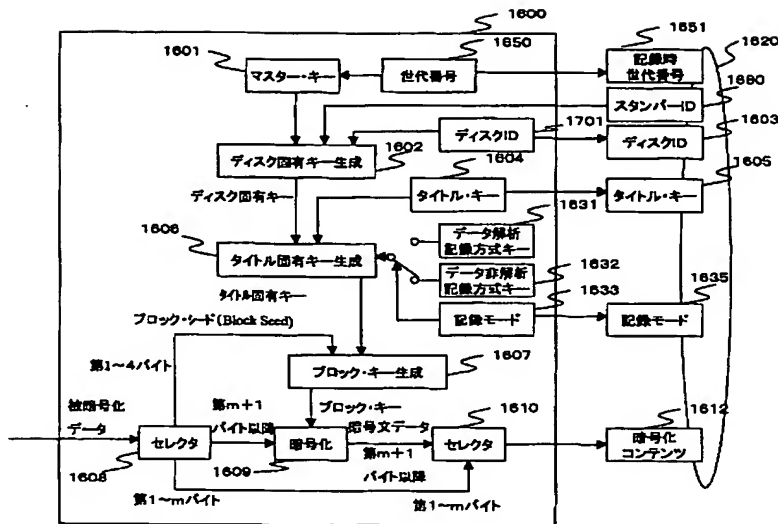
【図 16】



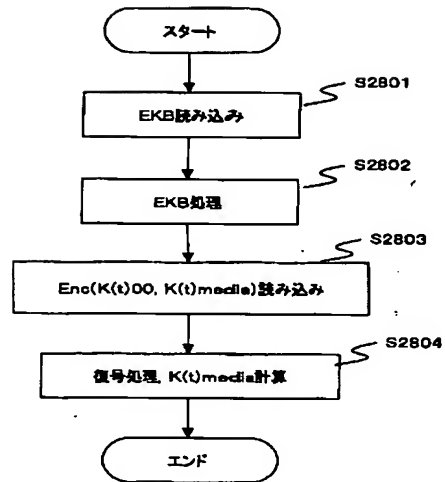
【図 3 2】



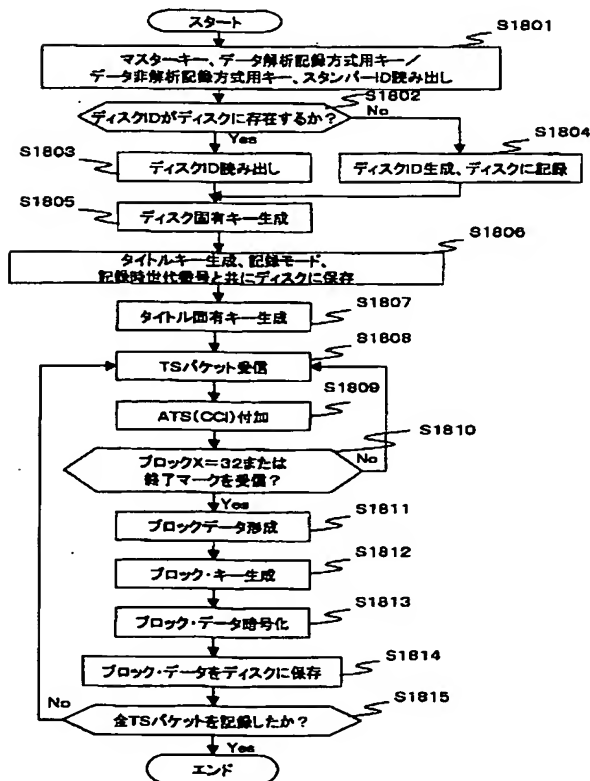
【図17】



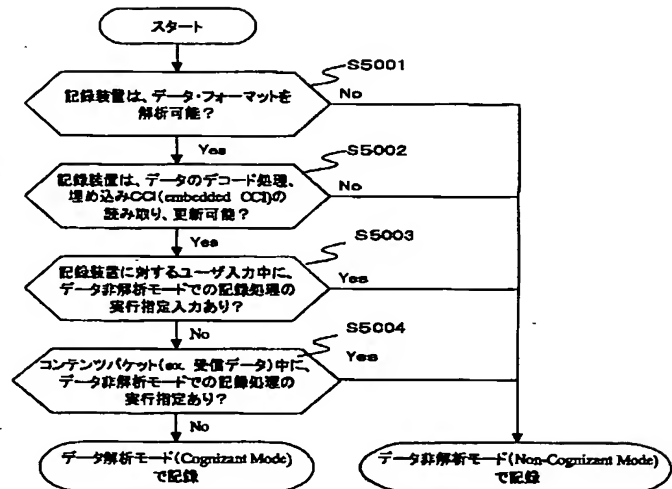
【図36】



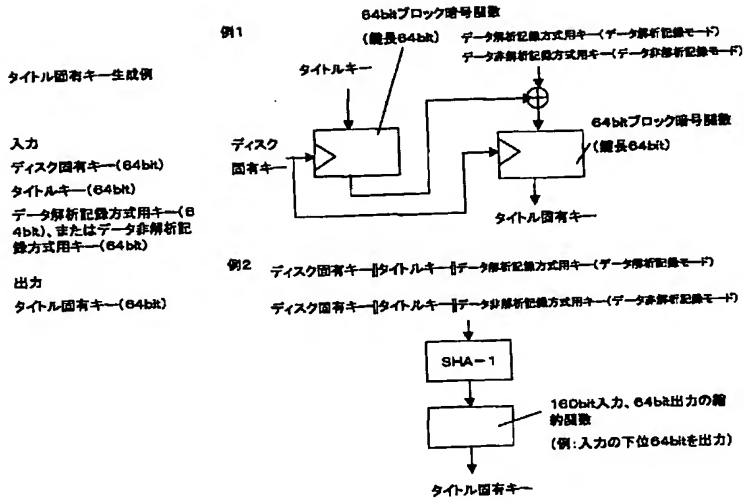
【図18】



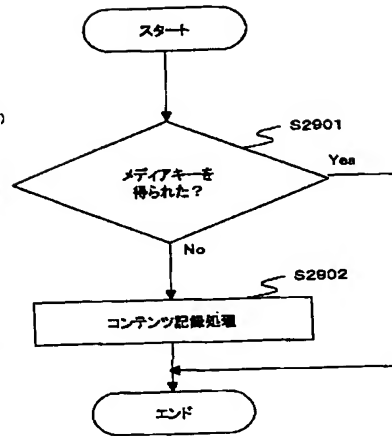
【図21】



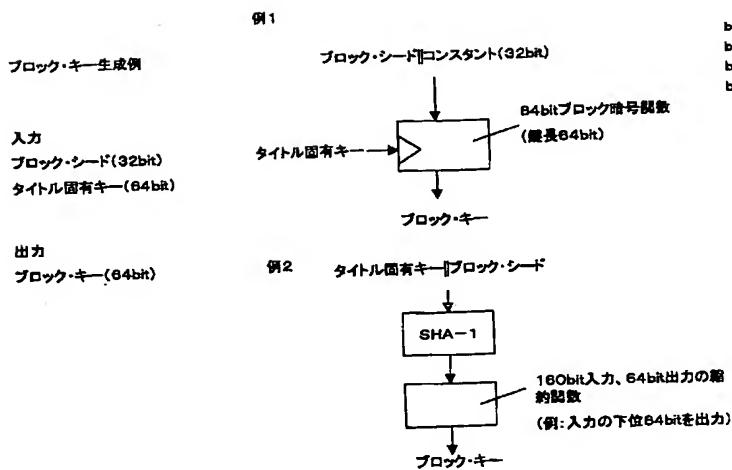
【図 22】



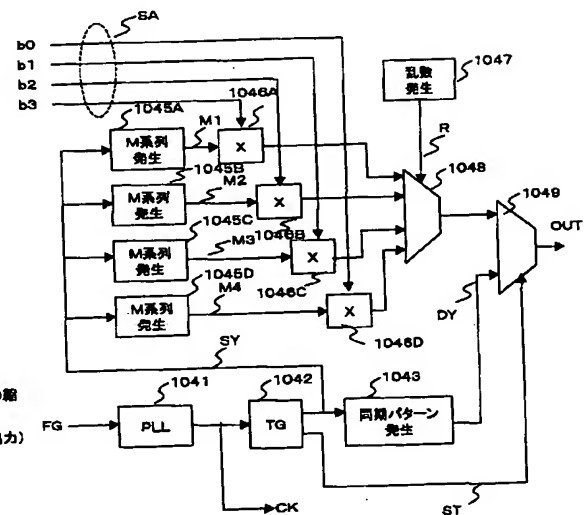
【図 37】



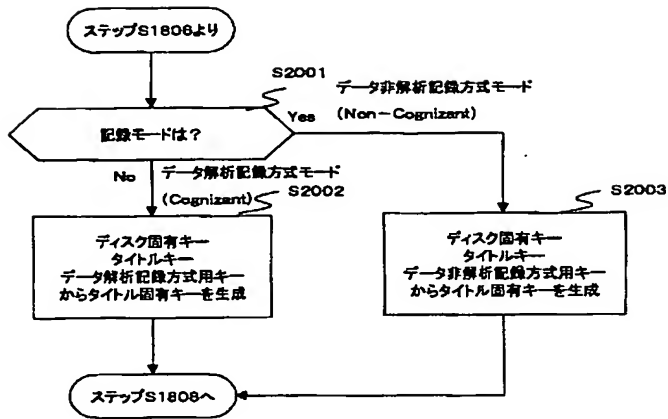
【図 23】



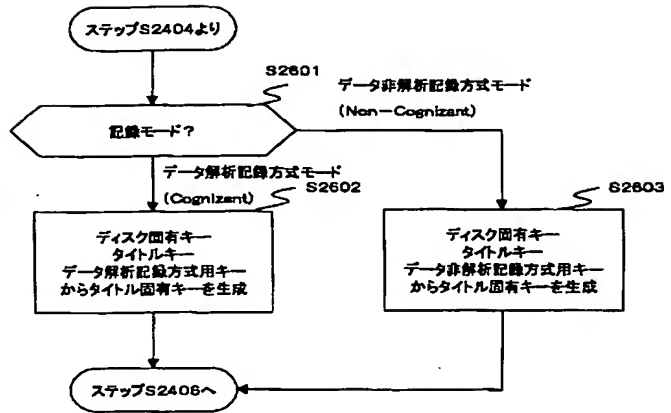
【図 25】



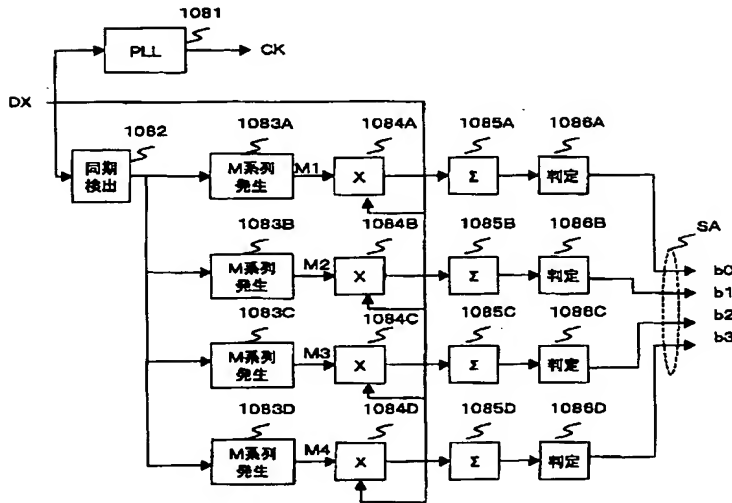
【図 24】



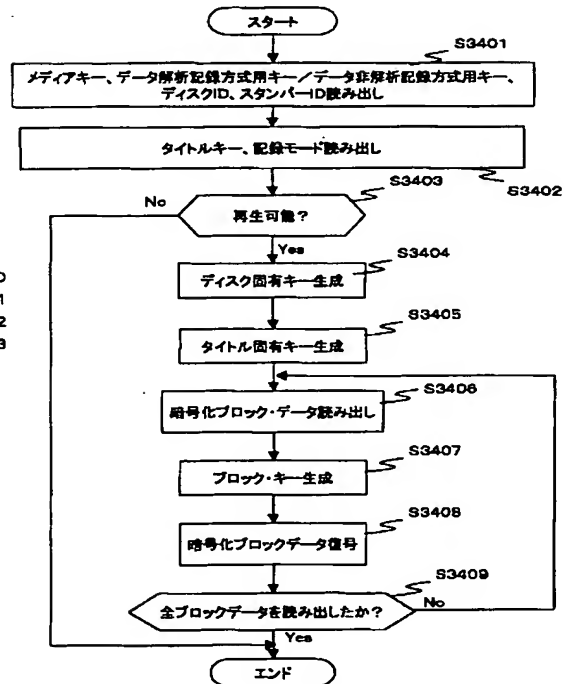
【図 34】



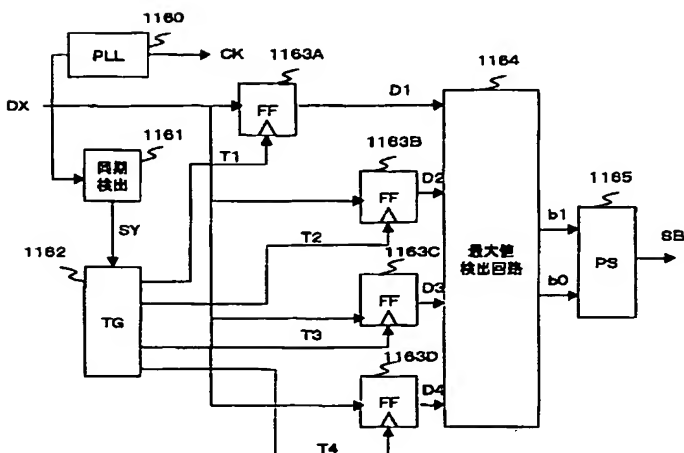
【図 26】



【図 42】



【図 28】



【图 48】

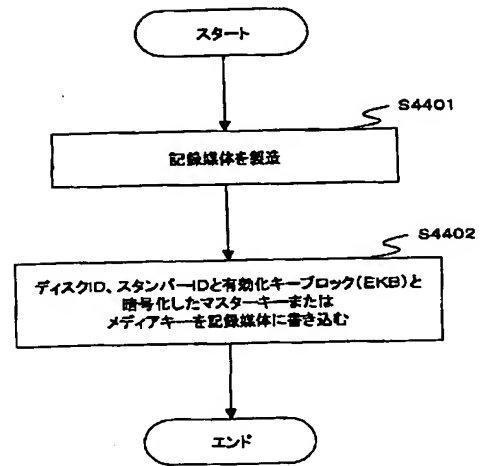
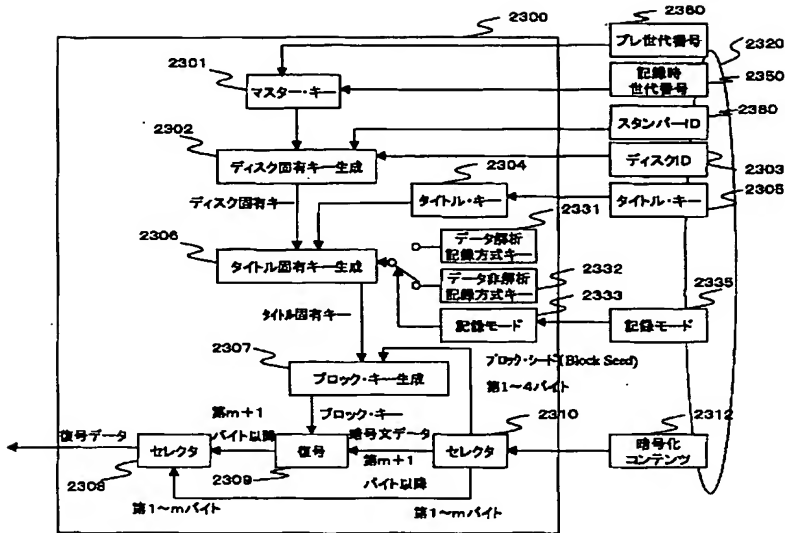


Figure 1 is a block diagram of the data encryption system. The diagram shows the flow from input data to encrypted output. Key components include:

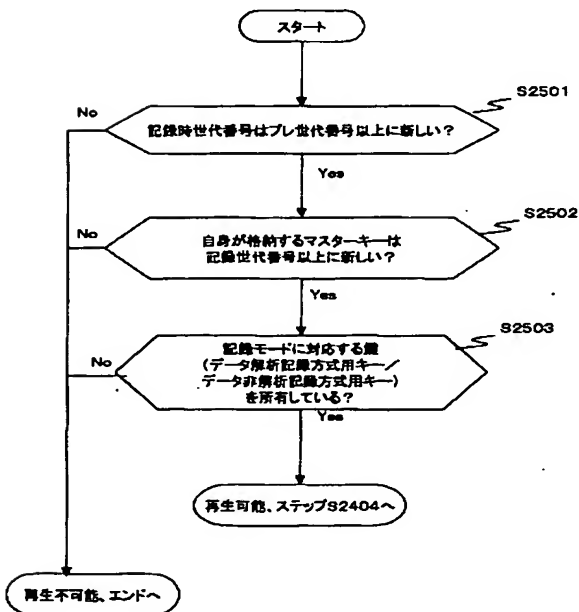
- 1601** Master Key
- 1650** Generation Number
- 1602** Disk Key Generation
- 1604** Title Key
- 1606** Title Key Generation
- 1607** Block Key Generation
- 1608** Data Encryption
- 1609** Decryption
- 1610** Selection
- 1612** Encrypted Content
- 1651** Encrypted Generation Number
- 1660** Encrypted Standby ID
- 1603** Encrypted Disk ID
- 1605** Encrypted Title Key
- 1632** Data Decompression/Encryption Method Key
- 1633** Recording Mode
- 1635** Recording Mode

The process involves generating keys from master and generation numbers, then using these keys to encrypt data in blocks.

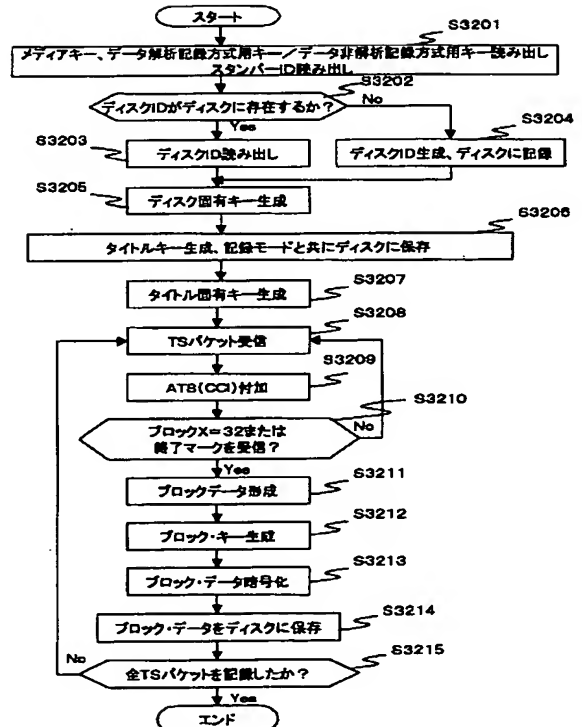
【図 31】



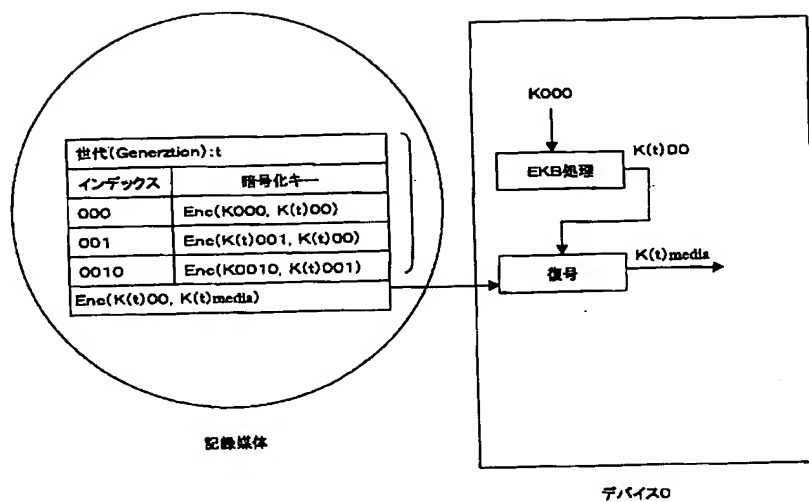
【図 33】



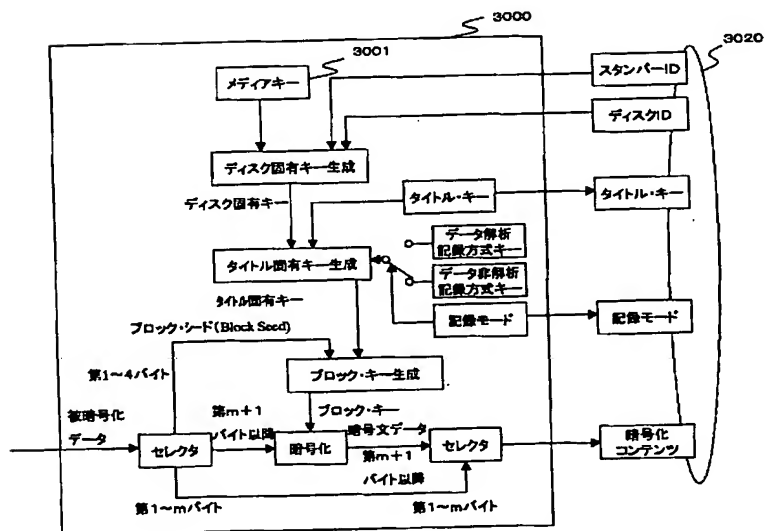
【図 40】



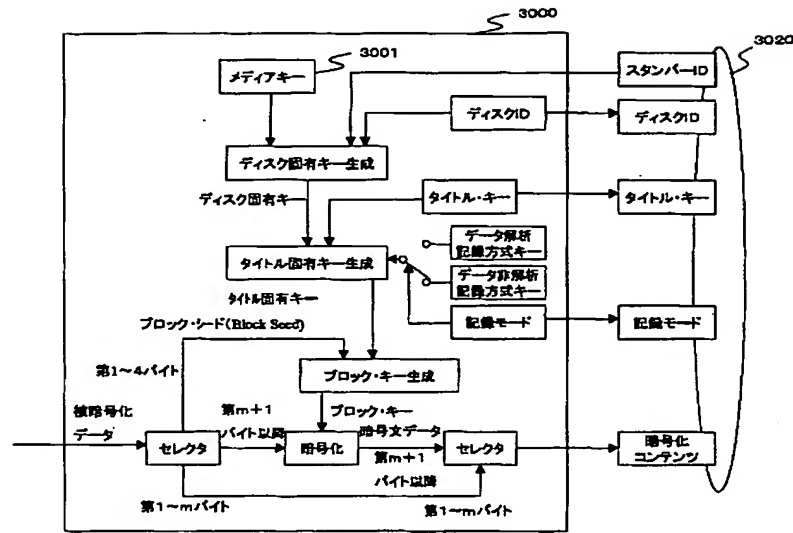
【図 35】



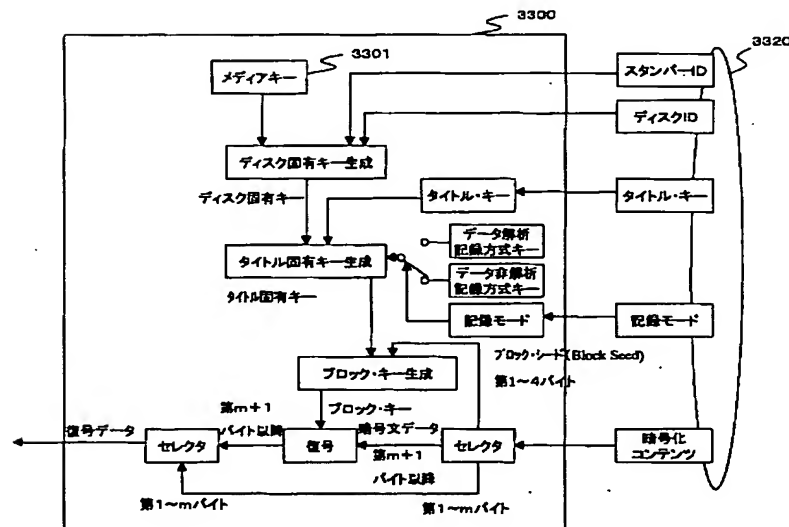
【図 38】



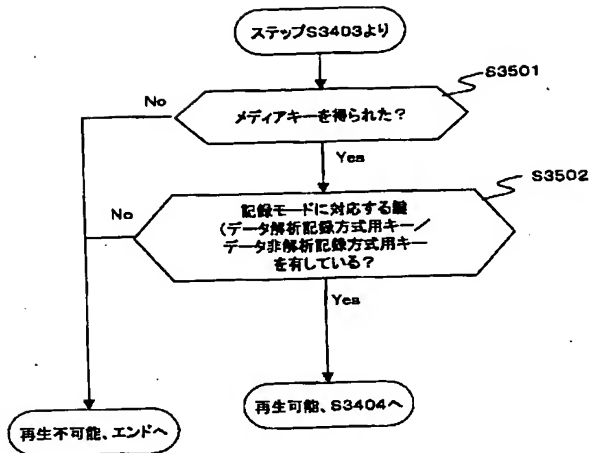
【図 39】



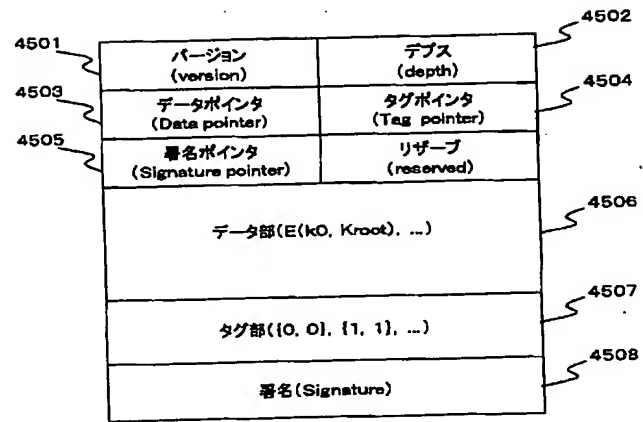
【図 41】



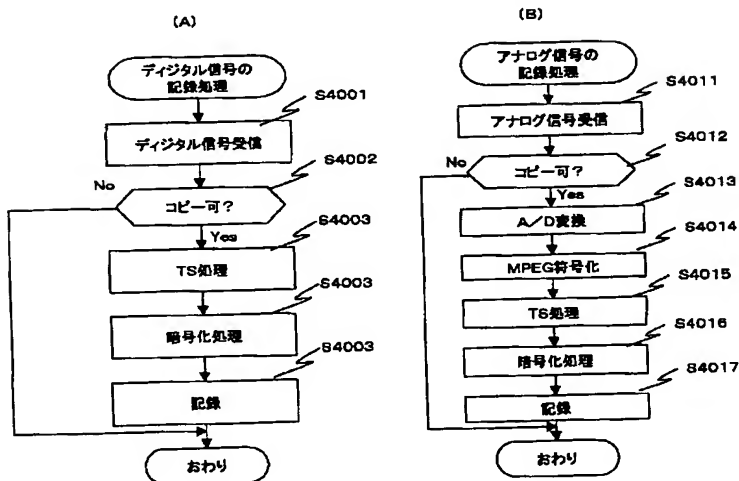
【図 43】



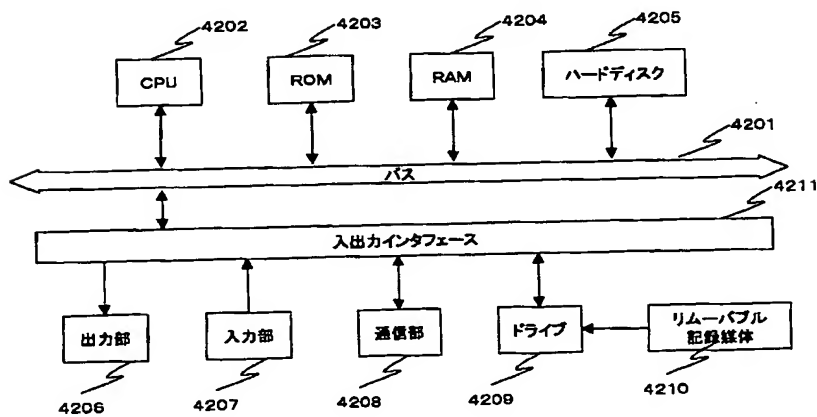
【図 49】



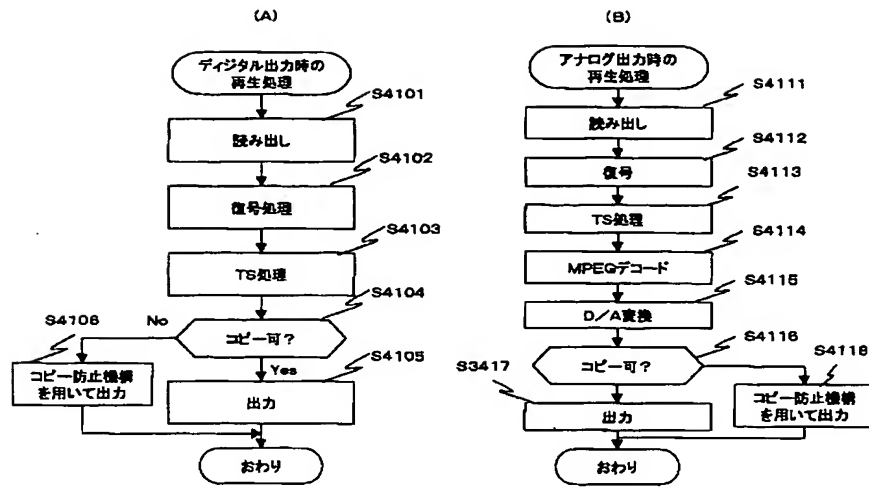
【図 44】



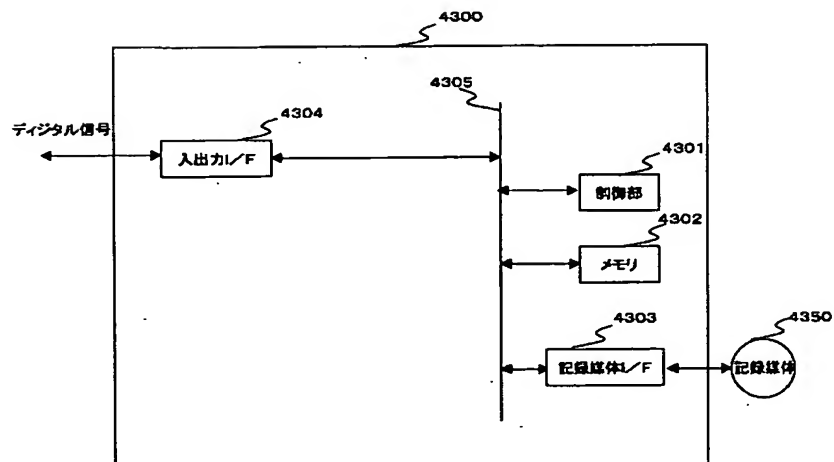
【図 46】



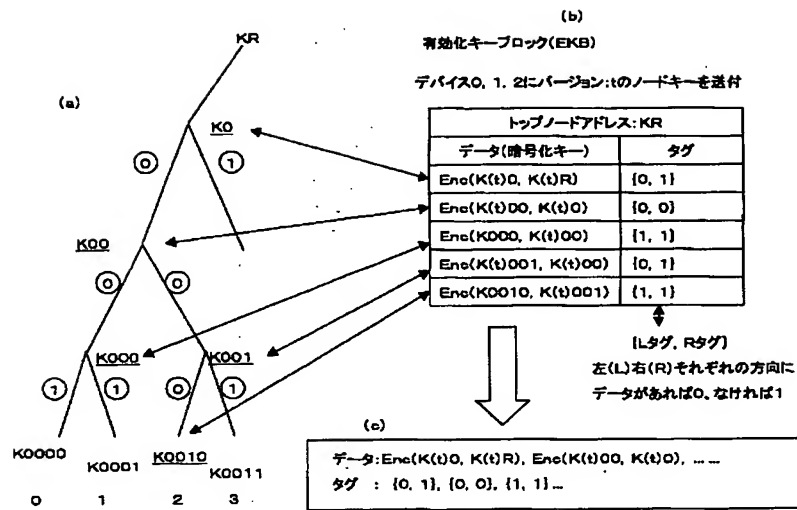
【図 45】



【図 47】

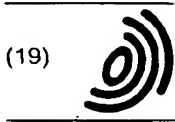


【図 50】



フロントページの続き

Fターム(参考) 5D044 AB01 AB05 AB07 BC02 CC04  
 EF05 FG18 GK17 HH13 HH15  
 HL06  
 5J104 AA01 AA12 AA16 EA04 EA26  
 JA03 MA08 NA02 NA31 NA32  
 PA14



Europäisches Patentamt  
European Patent Office  
Office européen des brevets



(11) EP 1 187 391 A2

(12) EUROPEAN PATENT APPLICATION

(43) Date of publication:  
13.03.2002 Bulletin 2002/11

(51) Int Cl.<sup>7</sup>: H04L 9/08, G11B 20/00

(21) Application number: 01307550.2

(22) Date of filing: 05.09.2001

(84) Designated Contracting States:  
AT BE CH CY DE DK ES FI FR GB GR IE IT LI LU  
MC NL PT SE TR  
Designated Extension States:  
AL LT LV MK RO SI

(72) Inventors:  
• Asano, Tomoyuki, c/o Intellectual Property  
Shinagawa-ku, Tokyo 141 (JP)  
• Osawa, Yoshitomo, c/o Intellectual Property  
Shinagawa-ku, Tokyo 141 (JP)

(30) Priority: 07.09.2000 JP 2000270919

(74) Representative: Pratt, Richard Wilson et al  
D. Young & Co,  
21 New Fetter Lane  
London EC4A 1DA (GB)

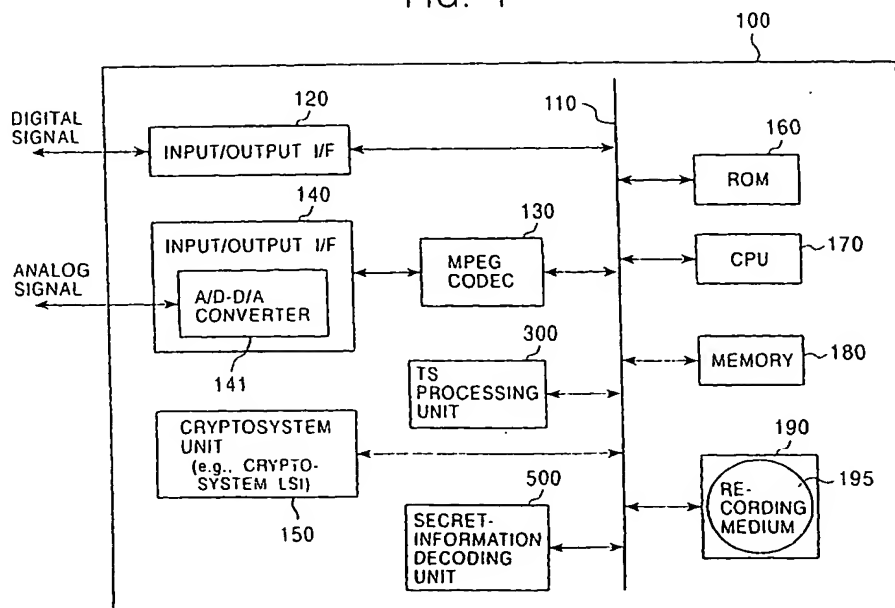
(71) Applicant: Sony Corporation  
Tokyo 141-0001 (JP)

(54) Encrypted information recording

(57) An information recording/playback device stores beforehand, on a recording medium, secret information in which a writing/reading method thereof cannot be analyzed and which can be read only by a special reading method. The secret information is applied to a key for content encryption or decryption when performing recording or playback of contents on the recording medium, such as music data and image data. The secret

information is, for example, a stamper ID. By using the stamper ID as secret information, and a master key and a media key which are distributed in a tree-structure key-distribution system, a content-cryptosystem key is generated. Accordingly, each content is allowed to be used in only an appropriate device in which the special reading method for the secret information can be executed and to which the key is distributed by the tree-structure key-distribution system.

FIG. 1



recording device. The decryption-key-generating data may be updated by using an enabling key block generated such that a node key is encrypted by using a key including at least one of a node key and a leaf key which are positioned at a lower level.

**[0032]** The decryption-key-generating data may be one of a master key common to a plurality of information recording devices and a media key unique to a specified recording medium.

**[0033]** The decryption-key-generating data may correspond to a generation number as updating information, and when storing encrypted data on the recording medium, the cryptosystem unit may store on the recording medium the generation number of the decryption-key-generating data as a recording-mode generation number.

**[0034]** The information playback device may further include a transport-stream processing unit for adding an arrival time stamp to each of transport packets constituting a transport stream. The cryptosystem unit may generate a block key as an encrypted key for block data composed of at least one transport packet to which the arrival time stamp is added, and in decryption of the data to be stored on the recording medium, the cryptosystem unit may generate a block key as a decryption key based on data including the secret information, the decryption-key-generating data, and a block seed as additional information which includes the arrival time stamp and which is unique to the block data.

**[0035]** The secret-information decoding unit may be structured to execute decoding processing on data which is stored on the recording medium by using a binary sequence to disturb a string of bits constituting the secret information, and the secret-information decoding unit may execute decoding processing of the secret information by generating the binary sequence and executing arithmetic processing using the generated binary sequence and a playback signal from the recording medium.

**[0036]** The secret-information decoding unit may read, from the recording medium, data which is recorded in a form converted in a predetermined manner from the secret information in units of a plurality of bits constituting the secret information, and may execute decoding processing on the secret information by converting the read data again.

**[0037]** According to a third aspect of the present invention, there is provided an information recording method for recording information on a recording medium, which includes a secret-information decoding step which reads secret information stored on the recording medium by executing a special data-reading process which is different from a process of reading content data stored on the recording medium, and a cryptosystem step which generates a content-encryption key by using, as a key-generating data, the secret information which is decoded after being read from the recording medium in the secret-information decoding step, and executes,

based on the content-encryption key, the encryption processing on the data to be stored.

**[0038]** The secret information may include a type of data among a stamper ID which is stored on the recording medium when the recording medium is produced and which is common to a plurality of recording media, a disk ID which is unique to each of the recording media, a content ID which is differently set for each content, and a cryptosystem key, and the secret-information decoding unit may execute a decoding process on the read data.

**[0039]** The cryptosystem step may include a step which uses the read secret information to generate the content-encryption key, and the read secret information is allowed to be used only in the generation of the content-encryption key which is executed in the cryptosystem step, without being stored in storage unit which is readable from the outside of the information recording device.

**[0040]** The cryptosystem step may include a step which generates the content-encryption key based on the read secret information and encryption-key-generating data which is stored in the information recording device, and the encryption-key-generating data may be updated by an enabling key block generated such that in a hierarchical tree structure having a plurality of different information recording devices as leaves, branches as nodes, and unique keys set for the leaves and the nodes, a node key is encrypted by using a key including at least one of a node key and a leaf key which are positioned at a lower level.

**[0041]** The encryption-key-generating data may be one of a master key common to a plurality of information recording devices and a media key unique to a specified recording medium.

**[0042]** The encryption-key-generating data may correspond to a generation number as updating information, and when storing encrypted data on the recording medium, the cryptosystem step may store on the recording medium the generation number of the encryption-key-generating data as a recording-mode generation number.

**[0043]** The information recording method may further include a transport-stream processing step for adding an arrival time stamp to each of transport packets constituting a transport stream. The cryptosystem step may include a step which generates a block key as an encrypted key for block data composed of at least one transport packet to which the arrival time stamp is added, and in encryption of the data to be stored on the recording medium, the cryptosystem step may generate a block key as an encryption key based on data including the secret information, the encryption-key-generating data, and a block seed as additional information which includes the arrival time stamp and which is unique to the block data.

**[0044]** The secret-information decoding step may include a step which executes decoding processing on

executed by the CPU 170, and data required for the operation of the CPU 170. By driving the recording medium 195, to/from which digital data can be recorded/played back, the drive 190 reads (plays back) and outputs digital data from the recording medium 195 to the bus 110, and supplies digital data supplied via the bus 110 so that the digital data is recorded on the recording medium 195. The device keys may be stored in the memory 180.

[0071] The recording medium 195 is a medium that can store digital data, for example, an optical disk such as digital versatile disk (DVD) or compact disk (CD), magneto-optical disk (MO), magnetic disk, magnetic tape, or semiconductor memory such as RAM. In this embodiment, the recording medium 195 can be loaded/unloaded into/from the drive 190. However, the recording medium 195 may be built into the recording/playback device 100.

[0072] The TS processing unit 300, which is fully described later with reference to Fig. 6 and the following drawings, performs data processing that, after extracting transport packets corresponding to a specified program from a transport stream in which a plurality of TV programs (contents) are multiplexed, stores appearance-timing information of the extracted transport packets on the recording medium 195, with each packet, and appearance-timing-control processing in the mode of reading from the recording medium 195.

[0073] In the transport stream, an arrival time stamp (ATS) is set as appearance-timing information of each transport packet. This timing is determined in an encoding mode so as not to break a transport stream system target decoder (T-STD) which is a virtual decoder defined in MPEG-2. When the transport stream is played back, an arrival time stamp that is added to each transport packet controls the appearance timing. The TS processing unit 300 executes control of these steps. For example, for recording a transport packet on the recording medium 195, the transport packet is recorded as a source packet in which intervals of packets are shortened. By recording the transport stream on the recording medium 195 with the appearance timing of each transport stream, the output timing of each transport packet can be controlled in playback mode. When recording data on the recording medium 195 such as DVD, the TS processing unit 300 additionally records an arrival time stamp representing the input timing of each transport packet.

[0074] The recording/playback device 100 according to an embodiment of the invention executes encryption of a content composed of a transport stream to which the arrival time stamp is added, and the encrypted content is stored on the recording medium 195. The cryptosystem unit 150 executes decoding on the encrypted content which is stored on the recording medium 195. The details of these processes are described later.

[0075] The secret-information decoding unit 500 is a processing unit that executes the reading and decoding of secret information which can be read by performing

a special reading process stored on the recording medium 195. The secret information stored on the recording medium 195 includes, for example, a stamper ID set for each stamper in disk production, a disk ID differently set for each disk, a content ID differently set for each content, and various identification data and cryptographic keys, such as keys for use in cryptosystem processing.

[0076] The secret-information decoding unit 500 reads and decodes the secret information stored on the recording medium 195, and transfers the decoded secret information to the cryptosystem unit 150. The cryptosystem unit 150 uses the secret information to generate a cryptographic key which is used when a content is recorded/read on/from the recording medium 195. The secret information, decoded by the secret-information decoding unit 500, is used only when a content-encryption key is generated in the cryptosystem unit 150, without being stored in a storage unit which is readable from the outside of the recording/playback device 100, so that the secret information is prevented from leaking to the exterior.

[0077] The cryptosystem unit 150, the TS processing unit 300, and the secret-information decoding unit 500 are shown as separate blocks for ease of understanding. However, the units 150, 300, and 500 may be formed as one or a plurality of LSIs that execute the functions of the units. Also, any of the functions may be implemented by combining software and hardware.

[0078] The construction shown in Fig. 2 can be used as an embodiment of a recording/playback device in addition to the construction shown in Fig. 1. In a recording/playback device 200 shown in Fig. 2, a recording medium 205 can be removably loaded into a recording medium interface (I/F) 210 as a drive unit, and data reading and writing can be performed, even if the recording medium 205 is loaded into another recording/playback device.

#### 40 Data-Recording Process and Data Reading Process

[0079] Next, with reference to the flowcharts shown in Figs. 3A to 4B, a process of recording data on the recording medium 195 and a process of playback of data from the recording medium 195 in the recording/playback device 100 or 200 in Fig. 1 or 2 are described below.

[0080] When a digital-signal content from the exterior is recorded on the recording medium 195, a recording process in accordance with the flowchart shown in Fig. 3A is performed.

[0081] Specifically, a digital-signal content (digital content) is supplied to the input/output I/F 120 via, for example, an IEEE (Institute of Electrical and Electronic Engineers) 1394 serial bus or the like, in step S301, the supplied content is received and output to the TS processing unit 300 via the bus 110.

[0082] In step S302, the TS processing unit 300 gen-

erates block data in which an arrival time stamp is added to each transport packet forming a transport stream, and outputs the block data to the cryptosystem unit 150 via the bus 110.

[0083] In step S303, the cryptosystem unit 150 executes encryption processing on the received content, and outputs the obtained encrypted content to the drive 190 or the recording medium I/F 210 via the bus 110. The encrypted content is recorded (step S304) on the recording medium 195 via the drive 190 or the recording medium I/F 210, and the recording process ends. The encryption processing in the cryptosystem unit 150 is described later.

[0084] Five companies including the assignee of the present Application, Sony Corporation, has established the Five Company Digital Transmission Content Protection (hereinafter referred to as the "5CDTCP" or "DTCP") system as a standard for protecting digital contents in a case in which the digital contents are transmitted between devices connected by an IEEE 1394 serial bus. In the DTCP, when a digital content having no copy-free information is transmitted between devices, authentication which determines whether or not copy-control information for copy control is properly treated is mutually performed before performing data transmission. After that, the digital content is encrypted and transmitted at a transmitting end, and the encrypted digital content (hereinafter referred to also as the "encrypted content") is decrypted at the receiving end.

[0085] In data transmission/reception based on the DTCP standard, in step S301, the input/output I/F 120 at the data receiving end receives the encrypted content via the IEEE 1394 serial bus. After decrypting the encrypted content in accordance with the DTCP standard, the input/output I/F 120 outputs the content as plaintext to the cryptosystem unit 150.

[0086] Digital content encryption based on the DTCP is performed by using a time-changing key after generating the key. The encrypted digital content is transmitted on the IEEE 1394 serial bus, including a key used for the encryption, and at the receiving end, the encrypted digital content is decrypted by using the key included therein.

[0087] According to the DTCP, accurately, an initial value of the key, and a flag representing timing of changing a key for use in encryption of the digital content are included in the digital content. At the receiving end, by changing the initial value of the key included in the encrypted content, based on the timing of the flag included in the encrypted content, a key used for encryption is generated and the encrypted content is decoded. Here, it may be considered that the encrypted content is equivalent to a case in which a key for decrypting the encrypted content is included therein. Concerning the DTCP, on a Web page specified by a uniform resource locator (URL) of, for example, <http://www.dtcp.com>, an information version can be obtained.

[0088] Next, with reference to the flowchart in Fig. 3B,

a case in which an analog signal content from the exterior is recorded on the recording medium 195 is described below.

[0089] When the analog signal content (hereinafter referred to also as the "analog content") is supplied to the input/output I/F 140, in step S321, the input/output I/F 140 receives the analog content. In step S322, the input/output I/F 140 generates a digital signal content (digital content) by using the A/D-D/A converter 141 to perform analog-to-digital conversion on the analog content.

[0090] The digital content is supplied to the MPEG codec 130. In step S323, the MPEG codec 130 performs MPEG encoding or encoding processing using MPEG compression on the digital content, and supplies the encoded content to the cryptosystem unit 150 via the bus 110.

[0091] After that, steps S324, S325, and S326 are performed identically to steps S302, S303, and S304 in Fig. 3A. In other words, the addition of an arrival time stamp to each transport packet by the TS processing unit 300 and the encryption processing by the cryptosystem unit 150 are performed. The resulted encrypted content is recorded on the recording medium 195, and the recording processing is terminated.

[0092] With reference to the flowcharts shown in Figs. 4A and 4B, processing in which a content recorded on the recording medium 195 is played back and output as a digital content or an analog content is described below.

[0093] A process of outputting the content as a digital content to the exterior is executed as a playback process in accordance with the flowchart in Fig. 4A. Specifically, in step S401, the encrypted content recorded on the recording medium 195 is read by the drive 190 or the recording medium I/F 210, and is output to the cryptosystem unit 150 via the bus 110.

[0094] In step S402, the cryptosystem unit 150 performs decryption processing on the encrypted content supplied from the drive 190 or the recording medium I/F 210, and outputs the decrypted data to the TS processing unit 300 via the bus 110.

[0095] In step S403, the TS processing unit 300 determines output timing from the arrival time stamp of each transport packet forming the transport stream, performs control in accordance with the arrival time stamp, and supplies the transport packet to the input/output I/F 120 via the bus 110. The input/output I/F 120 outputs the digital content from the TS processing unit 300 to the exterior and terminates the playback processing.

The processing of the TS processing unit 300 and the digital-content decoding processing of the cryptosystem unit 150 are described later.

[0096] In step S404, when outputting the digital content via the IEEE 1394 serial bus, the input/output I/F 120 performs mutual authentication with another device, as described above, and succeedingly transmits the digital content in an encrypted form.

[0097] When the content recorded on the recording

medium 195 is played back and output as an analog content to the exterior, a playback process in accordance with the flowchart in Fig. 4 is performed.

[0098] Specifically, steps S421, S422, and S423 are performed identically to steps S401, S402, and S403. These supply the MPEG codec 130 via the bus 110 with the decoded digital content obtained in the cryptosystem unit 150.

[0099] In step S424, the MPEG codec 130 performs MPEG decoding or decompression processing on the digital content, and supplies the decompressed content to the input/output I/F 140. In step S425, the input/output I/F 140 generates an analog content by using the built-in A/D-D/A converter 141 to perform digital-to-analog conversion on the MPEG-decoded digital content. In step S426, the input/output I/F 140 outputs the analog content to the exterior and terminates the playback process.

#### Data Format

[0100] Next, with reference to Fig. 5, a data format on the recording medium 195 in an embodiment of the invention is described below.

[0101] In the present invention, a minimum unit for reading/writing data from/on the recording medium 195 is called a "block". One block has a size of 192 by X bytes (e.g., X = 32).

[0102] In this embodiment of the invention, a 4-byte arrival time stamp is added to a 188-byte transport stream packet in accordance with MPEG-2 so that the total size is 192 bytes, and X ATS-added transport stream packets constitute one block of data. An arrival time stamp is data of 24 to 32 bits which represents an arrival time. An arrival time stamp is formed as random data in accordance with the arrival time of each packet. In one block (sector) of the recording medium 195, X ATS-added transport stream packets are recorded. In this illustrative embodiment of the invention, by using an arrival time stamp added to the first transport stream packet of each block forming a transport stream, a block key for encrypting the data of the block (sector) is generated.

[0103] By using the random arrival time stamp to generate the encryption block key, different unique keys for blocks are generated. The generated block unique keys are used to perform encryption processing on blocks. Also, by employing the ATS-used generation of the block keys, the need for the area of the recording medium 195 required for the encryption keys is eliminated, and a main data area can be effectively used. This eliminates the need for accessing data other than the main data in data recording and reading modes, so that efficient processing can be performed.

[0104] The block seed shown in Fig. 5 is additional information including the arrival time stamp. The block Seed may include not only the arrival time stamp but also copy control information (hereinafter referred to as

so as "CCI"). In this case, by using the arrival time stamp and the copy control information, each block key can be generated.

[0105] The copy control information included in the block seed, which is described later, is copy control information proposed as a joint proposal of five enterprises by the DTCP system. The copy control information reflects one of two types of information in accordance with device performance, namely, encryption mode indicator (EMI), and embedded CCI which is copy control information embedded in a content and which is applied to a format having a predetermined portion for sending copy control information.

[0106] In this embodiment of the invention, when data is stored on a recording medium such as a DVD, most of content data is encrypted, but first m bytes (e.g., m = 8 or 16) of the block are not encrypted and recorded as unencrypted data, and the remaining data (byte m+1 or greater) is encrypted, as is indicated by the bottom image in Fig. 5. This is because encrypted data length is restricted by performing the encryption processing in units of eight bytes. If the encryption processing can be performed not in units of eight bytes but in units of one byte, all portions excluding the block seed may be encrypted using m = 4.

#### Processing by TS Processing Unit 300

[0107] The function of the arrival time stamp is described below.

[0108] As described above, the arrival time stamp is added in order to store the appearance timing of each transport packet in an input transport stream.

[0109] Specifically, when one or more TV programs (contents) are extracted from a transport stream in which a plurality of TV programs (contents) are multiplexed, transport stream packets constituting the transport stream appear irregularly (see Fig. 7A). In the transport stream, the appearance timing of each transport packet has important meaning. The appearance timing is determined in encoding mode so as not to break a transport stream system target decoder (T-STD) which is a virtual decoder defined in MPEG-2 (ISO/IEC 13818-1).

[0110] When the transport stream is played back, the appearance timing is controlled by the arrival time stamp added to each transport packet. Accordingly, when recording transport packets on the recording medium 195, the input timing of each transport packet should be stored. Thus, when recording the transport packet on the recording medium 195, an arrival time stamp that represents the input timing of each transport packet is additionally recorded.

[0111] Fig. 6 is a block diagram illustrating processing executed by the TS processing unit 300 when a transport stream input via a digital interface is recorded on a storage medium as the recording medium 195. From a terminal 600, a transport stream is input as digital data

of digital broadcasting. In Fig. 1 or 2, the transport stream is input from the terminal 600 either via the input/output I/F 120 or via the input/output I/F 140 and the MPEG codec 130.

[0112] The transport stream is input to a bit stream parser 602. The bit stream parser 602 detects a program clock reference (PCR) packet from the input transport stream. The PCR packet is such that PCR defined in MPEG-2 is encoded. The PCR packet is obtained by performing encoding at time intervals of 100 milliseconds or less. The PCR represents a time at which a transport packet arrives at the receiving side, with precision of 27 MHz.

[0113] In a 27-MHz phase-locked loop (PLL) 603, the 27-MHz clock signal of the recording/playback device is locked in the program clock reference of the transport stream. A time stamp generating circuit 604 generates a time stamp based on a count of clocks of the 27-MHz clock signal. A block seed adding circuit 605 uses a time stamp obtained when the first byte of a transport stream is input to a smoothing buffer 606, as an arrival time stamp, and adds the arrival time stamp to the transport stream.

[0114] The ATS-added transport packet passes through the smoothing buffer 606 and is output from a terminal 607 to the cryptosystem unit 150. After the ATS-added transport packet is encoded by the cryptosystem unit 150, the encoded transport packet is recorded on the recording medium 195 as a storage medium via the drive 190 (Fig. 1) or the recording medium I/F 210 (Fig. 2).

[0115] Figs. 7A to 7C show an example of a process performed when the input transport stream is recorded on the recording medium 195. Fig. 7A shows input transport packets constituting a specified program (content), where the vertical axis is a time base indicating time on the transport stream. As shown in Fig. 7A, the input transport packets appear with irregular timing.

[0116] Fig. 7B shows an output from the block seed adding circuit 605. The block seed adding circuit 605 outputs source packets by adding, to each transport packet, a block seed including an arrival time stamp representing a time on the stream of the packets. Fig. 7C shows source packets recorded on the recording medium 195. By recording the source packets at shortened intervals as shown in Fig. 7C, the recording area of the recording medium 195 can be effectively used.

[0117] Fig. 8 shows a processing configuration of the TS processing unit 300 in a case in which the transport stream recorded on the recording medium 195 is played back. An ATS-added transport packet, decoded by a cryptosystem unit (described later), is input from a terminal 800 to a block seed separation circuit 801, and is separated into an arrival time stamp and a transport packet. A timing generating circuit 804 calculates a time based on a clock counter value of a 27-MHz clock unit 805 of the TS processing unit 300 when it performs playback.

[0118] At the start of playback, the first arrival time stamp is set as an initial value in a timing generating circuit 804. A comparator 803 compares the arrival time stamp with the present time input from the timing generating circuit 804. When the time generated by the timing generating circuit 804 is equal to the arrival time stamp, an output control circuit 802 outputs the transport packet to the MPEG codec 130 or the input/output I/F 120.

[0119] Fig. 9 is a block diagram showing a case in which an input AV signal is MPEG-encoded by the MPEG codec 130 of the recording/reproducing unit 100, and a transport stream is encoded by the TS processing unit 300. Accordingly, Fig. 9 is a block diagram showing a combination of the MPEG codec 130 and the TS processing unit 300 in Fig. 1 or 2.

[0120] A video signal is input from a terminal 901 to an MPEG video encoder 902.

[0121] The MPEG video encoder 902 encodes the input video signal to generate an MPEG video stream, and outputs the MPEG video stream to a video stream buffer 903. The MPEG video encoder 902 outputs access-unit information on the MPEG video stream to a multiplex scheduler 908. An access unit is a picture, and the access-unit information is the picture type of each picture, an amount of encoded bits, and a decode-time stamp. The picture type is I/P/B picture information. The decode-time stamp is information defined in MPEG-2.

[0122] An audio signal is input from a terminal 904 to an MPEG audio encoder 905. The MPEG audio encoder 905 encodes the input audio signal to generate an MPEG audio stream, and outputs the stream to an audio stream buffer 906. The MPEG audio encoder 905 also outputs access-unit information on the MPEG audio stream to the multiplex scheduler 908. An access unit of an audio stream is an audio frame, and the access-unit information is an amount of encoded bits in each audio frame and a decode-time stamp.

[0123] Access-unit information on video and audio is input to the multiplex scheduler 908. Based on the input access-unit information, the multiplex scheduler 908 controls a method of encoding a video stream and an audio stream to generate transport packets. The multiplex scheduler 908 includes a 27-MHz-precision clock generator for generating a reference time, and determines packet-encoding control information for a transport packet so as to satisfy a transport stream system target decoder as a virtual decoder model. The packet-encoding control information is a type of a stream to be formed in packet and the length of a stream.

[0124] When the packet-encoding control information represents a video packet, a switch 976 connects to the side a, so that video data is read which has a payload data length designated by the packet-encoding control information from the video stream buffer 903, and is input to a transport packet encoder 909.

[0125] When the packet-encoding control information represents an audio packet, the switch 976 connects to

the side b, so that audio data is read which has a payload data length designated by the audio stream buffer 906, and is input to the transport packet encoder 909.

[0126] When the packet-encoding control information represents a program clock reference packet, the transport packet encoder 909 captures a program clock reference input from the multiplex scheduler 908, and outputs a program clock reference packet. When the packet-encoding control information indicates that packet encoding is not performed, nothing is input to the transport packet encoder 909.

[0127] When the packet-encoding control information indicates that packet encoding is not performed, the transport packet encoder 909 does not output any transport packet. In cases other than that, based on the picture, the transport packet encoder 909 generates and outputs transport packets. Accordingly, the transport packet encoder 909 intermittently outputs transport packets. Based on the program clock reference input from the multiplex scheduler 908, an arrival time stamp calculator 910 calculates, an arrival time stamp representing a time at which the first byte of the transport packet arrives at the receiving side.

[0128] The program clock reference input from the multiplex scheduler 908 represents an arrival time at which the tenth byte of a transport packet defined in MPEG-2 arrives at the receiving side. Thus, the value of the arrival time stamp is an arrival time of a byte that is positioned ten bytes before the time of the program clock reference.

[0129] A block-seed adding circuit 911 adds an arrival time stamp (ATS) to the transport packet output from the transport packet encoder 909. The ATS-added transport packet which is output from the block-seed adding circuit 911 passes through a smoothing buffer 912 to be input to the cryptosystem unit 150. After the input ATS-added transport packet is encrypted as described later, the encrypted ATS-added transport packet is recorded on the recording medium 195 as a storage medium.

[0130] Before being encrypted by the cryptosystem unit 150, the ATS-added transport packets to be recorded on the recording medium 195 are input, with the intervals of the packets shortened. After that, the encrypted ATS-added transport packets are recorded on the recording medium 195. Even if transport packets are recorded with the intervals thereof shortened, a time at which the transport packets are input can be controlled.

[0131] The length of an arrival time stamp is not limited to 32 bits, but may be 24 to 31 bits. The longer the bit length of the arrival time stamp, the greater each cycle of a time counter for arrival time stamp. For example, when the time counter for arrival time stamp is a binary counter with precision of 27 MHz, the time required for a cycle of a 24-bit-length arrival time stamp is approximately 0.06 seconds. This time is sufficient for an ordinary transport stream. This is because under provision of MPEG-2, each packet interval of transport streams is a maximum of 0.1 seconds. However, the arrival time

stamp may have 24 or more bits for sufficient tolerance.

[0132] In the above cases in which the bit length of the arrival time stamp is variously set, there are a plurality of possible configurations for a block seed as an additional data to block data.

[0133] Fig. 10 shows block seed configurations. In example 1 in Fig. 10, thirty-two bits are used for the arrival time stamp. In example 2 in Fig. 10, thirty bits are used for the arrival time stamp, and two bits are used for copy control information. Copy control information represents a state of copy control in data to which the copy control information is added. Concerning copy control information, the Serial Copy Management System (SCMS) and the Copy Generation Management System (CGMS) are famous. By using copy control information based on these systems, types of information can be shown, such as "Copy Free" information indicating that data to which Copy Free information is added may be limitlessly copied, "One Generation Copy Allowed" information indicating that the copying of data to which One Generation Copy Allowed information is added can be performed only in one generation, and "Copy Prohibited" information indicating that the copying of data to which Copy Prohibited information is added is prohibited.

[0134] In example 3 in Fig. 10, twenty-four bits are used for the arrival time stamp, two bits are used for the copy control information, and six bits are used for other information. Various types of information, such as information representing the switching on/off of a Macrovision as an analog-picture-copy-control mechanism in a case in which other-information-included data is analog-output, can be used as other information.

#### Tree Structure as Key Distribution Configuration

[0135] Next, a configuration is described below in which the recording/playback device 100 or 200 in Fig. 1 or 2 distributes, to each device, the master key required for recording data on a recording medium or for playing back data from the recording medium 195.

[0136] Fig. 11 illustrates the distribution of a key for each recording/playback device in a recording system using the configuration. In Fig. 11, the numbers 0 to 15 shown at the bottom indicate recording/playback devices, respectively. The leaves of the tree structure shown in Fig. 11 correspond to the devices.

[0137] Each of the devices 0 to 15 stores node keys assigned to nodes from its leaf as a node to the root, and a leaf key corresponding to its leaf. The alphanumeric representations K0000 to K1111 shown in the bottom of Fig. 11 are leaf keys assigned to the devices 0 to 15. In Fig. 11, the top node KR to the nodes K000 to K111 in the second row from the bottom are node keys.

[0138] In the tree structure shown in Fig. 11, for example, device 0 possesses leaf key K0000, and node keys K000, K00, K0, and KR. Device 5 possesses leaf key K0101, and node keys K010, K01, K0, and KR. Device 15 possesses leaf key K1111, and node keys K111,

K11, K1, and KR. Although the tree structure shown in Fig. 11 includes only the sixteen devices 0 to 15 and has four levels and balanced symmetry, it may include more devices and a different number of levels in each portions of the tree.

[0139] The devices 0 to 15 as recording/playback devices include various types of recording/playback devices that use various types of recording media such as DVDs, CDs, MDs, and Memory Sticks (trademark). Also, it is possible that various application services coexist. The key distribution in Fig. 11 is applied to a configuration in different devices and different applications coexist.

[0140] In this system in which various devices and applications coexist, for example, the portion surrounded by the dotted line in Fig. 11, specifically, devices 0, 1, 2, and 3 are treated as a group using a single recording medium. To devices 0, 1, 2, and 3 included in this group, a process of simultaneously sending by a provider a common content in an encrypted form, a process of sending a master key for use in common, and a process of outputting content-charge-payment data in an encrypted form from each device to a provider are performed. An authority that transmits/receives data to/from each device, such as a content provider or a settlement authority, treats the portion surrounded by the dotted line in Fig. 11 as one group and performs simultaneous data-transmission processing. Similar groups exist in the tree in Fig. 11.

[0141] Node keys and leaf keys may be controlled by a single key, or may be controlled for each group by an authority that transmits/receives data to/from each group, such as a provider or a settlement authority. These node keys and leaf keys are updated, for example, when a leak of a key occurs, and the process of updating is executed by a key-control center, a provider, a settlement authority, etc.

[0142] As is clear from Fig. 11, in the tree structure, the three devices 0, 1, 2, and 3 included in one group possess common keys K00, K0, and KR as node keys. By using this node-key sharing system, for example, a common master key can be provided to a limited number of devices 0, 1, 2, and 3. For example, by using node key K00 itself, which is possessed in common, as a master key, only devices 0, 1, 2, and 3 can use the master key in common without receiving a new key. In addition, by distributing, to devices 0, 1, 2, and 3, code  $\text{Enc}(K00, K_{\text{master}})$  obtained by encrypting new master key  $K_{\text{master}}$  using node key K00 via a network or by using a recording medium containing the value, only devices 0, 1, 2, and 3 decrypt code  $\text{Enc}(K00, K_{\text{master}})$  with shared master key K00, which is possessed by them, and can obtain  $K_{\text{master}}$ . Data obtained by using  $K_a$  to encrypt  $K_b$  is represented by  $\text{Enc}(K_a, K_b)$ .

[0143] When it is discovered at time "t" that the keys of device 3, K0011, K001, K00, K0, and KR have been analyzed and exposed by a hacker, device 3 must be cut off from the system in order to protect data transmit-

ted and received in the system (the group of devices 0, 1, 2, and 3) after time "t". Accordingly, node keys K001, K00, K0, and KR should be updated to generate new keys  $K(t)001$ ,  $K(t)00$ ,  $K(t)0$ ,  $K(t)R$ , respectively, and the new keys should be posted to devices 0, 1, 2, and 3. Here,  $K(t)aaa$  represents an updated key in generation "t" of key Kaaa.

[0144] A process for distributing the updated keys is described below.

[0145] Key updating is performed by distributing, to devices 0, 1, and 2, a table formed by block data called an "enabling key block (EKB)" (shown in Fig. 12A), for example, via a network or by using recording media containing the table.

[0146] In the enabling key block shown in Fig. 12A, only devices in which node keys should be updated are shown as block data having an updatable data arrangement. The example shown in Fig. 12A is block data formed for the purpose of distributing updated node keys in generation "t" in connection with devices 0, 1, and 2 in the tree structure in Fig. 11. As is clear from Fig. 11, devices 0 and 1 need  $K(t)00$ ,  $K(t)0$ , and  $K(t)R$  as updated keys, device 2 needs  $K(t)001$ ,  $K(t)00$ ,  $K(t)0$ , and  $K(t)R$  as updated keys.

[0147] As the enabling key block in Fig. 12A shows, the enabling key block includes a plurality of encryption keys. The bottom encrypted key is  $\text{Enc}(K0010, K(t)001)$ . This is updated node key  $K(t)001$  obtained by performing encryption using leaf key K0010 of device 2. Device 2 can obtain  $K(t)001$  by using its own leaf key to decrypt encrypted key  $\text{Enc}(K0010, K(t)001)$ . By using  $K(t)001$  obtained by decryption, the second encrypted key  $\text{Enc}(K(t)001, K(t)00)$  from the bottom in Fig. 12A can be decrypted. This makes it possible to obtain updated node key  $K(t)00$ .

[0148] Similarly, by decrypting the second encrypted key  $\text{Enc}(K(t)00, K(t)0)$  from the top in Fig. 12A, updated node key  $K(t)0$  can be obtained. By decrypting the first encrypted key  $\text{Enc}(K(t)0, K(t)R)$  from the top in Fig. 12A,  $K(t)R$  can be obtained.

[0149] In the case of devices 0 and 1, node key K000 is not included in what to update. Necessary node keys are  $K(t)00$ ,  $K(t)0$ , and  $K(t)R$ . In devices 0 and 1, by decrypting the third encrypted key  $\text{Enc}(K000, K(t)00)$ ,  $K(t)00$  can be obtained.

[0150] Subsequently, by decrypting the second encrypted key  $\text{Enc}(K(t)00, K(t)0)$  from the top in Fig. 12A, updated node key  $K(t)0$  can be obtained. By decrypting the top encrypted key  $\text{Enc}(K(t)0, K(t)R)$ ,  $K(t)R$  can be obtained.

[0151] By using the above operation, devices 0, 1, and 2 can obtain updated key  $K(t)R$ . The "INDEX" in Fig. 12A indicates the absolute address of a node key or a leaf key used as a decryption key.

[0152] In a case in which upper node keys K0 and K01 in the tree structure in Fig. 11 do not need to be updated, and only node key K00 should be updated, updated node key  $K(t)00$  can be distributed to devices 0, 1, and

2 by using the enabling key block in Fig. 12B.

[0153] The enabling key block in Fig. 12B can be used in the case of distributing a new master key that is shared in a specified group. It is assumed as a specific example that devices 0, 1, 2, and 3 in the dotted-line group in Fig. 11 use certain recording media and need new common master key  $K(t)_{\text{master}}$ . Then, data  $\text{Enc}(K(t), K(t)_{\text{master}})$  is distributed which is obtained by encrypting updated master key  $K(t)_{\text{master}}$  with  $K(t)00$  obtained by updating node key  $K00$  common to devices 0, 1, 2, and 3. Thus, data  $\text{Enc}(K(t), K(t)_{\text{master}})$  is distributed, as data that is not decrypted, to the devices of other groups, such as device 4.

[0154] In other words, devices 0, 1, and 2 can obtain master key  $K(t)_{\text{master}}$  at time "t" by decrypting the above data using  $K(t)00$  obtained by processing the enabling key block.

#### Distribution of Master Key Using Enabling Key Block

[0155] Fig. 13 shows, as a processing example of obtaining master key  $K(t)_{\text{master}}$  at time "t", processing of device 0 that receives, via a recording medium, data  $\text{Enc}(K(t)00, K(t)_{\text{master}})$  obtained by using  $K(t)00$  to encrypt new common master key  $K(t)_{\text{master}}$ , and the enabling key block shown in Fig. 12B. As shown in Fig. 13, device 0 generates node key  $K(t)00$  by performing enabling-key-block processing similar to the above, using the enabling key block at time as a generation recorded on the recording medium. After decrypting updated master key  $K(t)_{\text{master}}$  using decrypted updated node key  $K(t)00$ , device 0 encrypts the master key using its own leaf key  $K0000$  and records the encrypted master key so that the master key can be used afterward. When device 0 can securely store updated master key  $K(t)_{\text{master}}$ , the encryption using leaf key  $K0000$  is not required.

[0156] With reference to the flowchart shown in Fig. 14, a process for acquiring the updated master key is described below. It is assumed that the latest master key  $K(c)_{\text{master}}$  is given to each recording/playback device when it is shipped and is stored in an internal memory securely (specifically, for example, in a form in which the given master key is encrypted using the device's leaf key).

[0157] When the recording medium that contains updated master key  $K(n)_{\text{master}}$  and the enabling key block is loaded into the recording/playback device, in step S1401, the recording/playback device reads the time (generation) number "n" (represented by pre-recording generation information #n) of the recorded master key  $K(n)_{\text{master}}$  from the recording medium. On the recording medium, the time (generation) number "n" of the recorded master key  $K(n)_{\text{master}}$  is recorded beforehand. In step S1402, after reading self-retained encryption master key C, the recording/playback device compares the "generation c" of the encryption master key and the "generation n" of the pre-recording generation information, and determines the order of the generations.

[0158] In step S1402, if the recording/playback device has determined that "generation n" represented by pre-recording generation information #n does not follow (is not newer than) the "generation c" of encrypted master key C stored in the internal memory, in other words, when the "generation c" of encrypted master key C is identical to or follows "generation n" represented by pre-recording generation information #n, steps S1403 to S1408 are skipped and the master key updating process is terminated. In this case, the master key  $K(c)_{\text{master}}$  stored in the internal memory is not updated since it does not need to be updated.

[0159] In step S1402, if the recording/playback device has determined that "generation n" represented by pre-recording generation information #n follows (is newer than) the "generation c" of encrypted master key C stored in the internal memory, in other words, when the "generation c" of encrypted master key C is older than "generation n" represented by pre-recording generation information #n, the recording/playback device proceeds to step S1403 and reads the enabling key block from the recording medium.

[0160] In step S1404, the recording/playback device calculates key  $K(t)00$  of node K00 at pre-recording generation information #n by using the enabling key block read in step S1403, and the leaf key ( $K0000$  in device 0 in Fig. 11) and the node keys ( $K000$ ,  $K00$ , etc., in device 0 in Fig. 11) which are stored in the internal memory.

[0161] In step S1405, the recording/playback device determines whether it has obtained  $K(t)00$  in step S1404. If the recording/playback device has not obtained  $K(t)00$ , it is indicated that the recording/playback device is revoked from the group in the tree structure that time. Accordingly, steps S1406 to S1408 are skipped and the master key updating process is terminated.

[0162] If the recording/playback device has obtained  $K(t)00$ , it proceeds to step S1406 and reads, from the recording medium,  $\text{Enc}(K(t)00, K(t)_{\text{master}})$ , which is a code obtained by using  $K(t)00$  to encrypt the master key at time "t". In step S1407, the recording/playback device uses  $K(t)00$  to decrypt the code and calculates  $K(t)_{\text{master}}$ .

[0163] In step S1408, in the recording/playback device,  $K(t)_{\text{master}}$  is encrypted using its leaf key ( $K0000$  in device 0 in Fig. 11) and is stored in the internal memory. After that, the master key updating process ends.

[0164] Although master keys are used in ascending order from the key at time (generation) zero (0), it is preferable that the master keys from the new generation to the older generation be structured by computation, as required by the component units of the system. In other words, the recording/playback device retains unidirectional "function f", and creates a desired master key by applying its own master key to the unidirectional "function f" a number of times which corresponds to the difference between the generation of the master key and the generation of the required master key.

[0165] Specifically, by way of example, when the generation of the master key MK stored in the recording/playback device is  $i+1$ , and the generation of the master key MK required for reading data is  $i-1$ , master key  $K(i-1)_{\text{master}}$  is generated such that in the recording/playback device, unidirectional "function  $f$ " is used twice to calculate  $f(f(K(i+1)_{\text{master}}))$ .

[0166] When the generation of the master key MK stored in the recording/playback device is  $i+1$ , and the generation of the master key MK required for reading data is  $i-2$ , master key  $K(i-2)_{\text{master}}$  is generated such that in the recording/playback device, unidirectional "function  $f$ " is used three times to calculate  $f(f(f(K(i+1)_{\text{master}})))$ .

[0167] In this operation, for example, the hash function can be used as the unidirectional "function  $f$ ". Specifically, MD5 (Message Digest 5), SHA-1 (Secure Hash Algorithm -1), etc., can be employed. A key issuing authority uses these unidirectional functions to beforehand calculate master keys by which generations older than their generations can be formed, namely,  $K(0)_{\text{master}}$ ,  $K(1)_{\text{master}}$ ,  $K(2)_{\text{master}}$ , ...,  $K(N)_{\text{master}}$ . Specifically, initially, by setting  $N$ -generating master key  $K(N)_{\text{master}}$ , and applying the unidirectional function to master key  $K(N)_{\text{master}}$  for each time, older generation master keys,  $K(N-1)_{\text{master}}$ ,  $K(N-2)_{\text{master}}$ , ...,  $K(1)_{\text{master}}$ ,  $K(0)_{\text{master}}$  are sequentially generated. After that, the generated master keys are used in sequence from smaller generation master key  $K(0)_{\text{master}}$ . It is assumed that unidirectional function that is used to generate master keys having generations older than the generation of a master key be set in all recording/playback devices.

[0168] Also, for example, public key cryptosystem technology can be used as a unidirectional function. In this case, a key issuing authority possesses a secret key for a public key cryptosystem and provides a public key corresponding to the secret key to all reproducing devices. The key issuing authority sets zero-th generation master key  $K(0)_{\text{master}}$ , and begins to use  $K(0)_{\text{master}}$ . Specifically, when requiring master key  $K(i)_{\text{master}}$  subsequent to the first generation, the key issuing authority generates and uses master key  $K(i)_{\text{master}}$  by using the secret key to convert master key  $K(i-1)_{\text{master}}$  which is older one generation. In this case, the key issuing authority does not need to generate an  $N$ -th generation master key beforehand by using the unidirectional function. According to this method, theoretically, master keys of a limitless number of generations can be generated. If each recording/playback device retains a master key of a generation, it can obtain a master key of a generation older than the generation by using a public key to convert the master key.

[0169] Next, with reference to the flowchart shown in Fig. 15, a process by the recording/playback device is described below which is performed when the recording/playback device records a content on its own recording medium.

[0170] Content data is encrypted using a master key of a generation and is distributed from a content provider to each recording/playback device via a network or using recording media.

[0171] In step S1501, the recording/playback device reads pre-recording generation information # $n$  from the recording medium. The recording/playback device also acquires the "generation  $c$ " of encrypted master key  $C$  stored in its own memory.

[0172] In step S1502, the recording/playback device compares the "generation  $c$ " of the encrypted master key  $C$  and "generation  $n$ " represented by pre-recording generation information # $n$ , and determines the order of the generations.

[0173] In step S1502, if the recording/playback device has determined that the "generation  $c$ " of encrypted master key  $C$  stored in its own memory does not follow "generation  $n$ " represented by pre-recording generation information # $n$ , in other words, when the "generation  $c$ " of encrypted master key  $C$  stored in its own memory is older than "generation  $n$ " represented by pre-recording generation information # $n$ , the recording/playback device skips over step S1503 and does not perform a content data recording process.

[0174] In step S1502, if the recording/playback device has determined that the "generation  $c$ " of encrypted master key  $C$  stored in its own memory follows "generation  $n$ " represented by pre-recording generation information # $n$ , in other words, when the "generation  $c$ " of encrypted master key  $C$  stored in its own memory is identical to or newer than "generation  $n$ " represented by pre-recording generation information # $n$ , the recording/playback device goes to step S1503 and performs the content data recording.

#### Content Data Encryption and Recording Processing Using Generation-Controlled Master Keys

[0175] A process in which a recording/playback device performs encryption of content data using generation-controlled master keys and records the encrypted data on its own recording medium is described below. Here, a process is described in which a block key is generated based on data using the generation-controlled master key, and data composed of the above transport stream is encrypted using the block key and is stored on a recording medium.

[0176] With reference to the block diagrams shown in Figs. 16 and 17, and the flowchart shown in Fig. 18, the above process is described below.

[0177] An optical disk is used as an example of a recording medium. In the embodiment shown in Figs. 16 to 18, in order to prevent the copying of data on the recording medium bit by bit, disk ID that is identification information unique to the recording medium is controlled to operate on a key for encryption of data.

[0178] In accordance with Figs. 16 and 17, an outline of data-encryption processing performed by the crypto-

system unit 150 is described below.

[0179] A recording/playback device 1600 reads a master key 1601, an analyzing data-recording key (hereinafter referred to as a "cognizant key") 1631 or a non-analyzing data-recording key (hereinafter referred to as a "noncognizant key") 1632, which are stored in an internal memory like the memory 180 (Fig. 1 or 2). The cognizant key 1631 and the non-cognizant key 1632 are described later.

[0180] The master key 1601 is a secret key stored in the memory of the recording/playback device 1600 as shown in the flow of Fig. 14. The generation of the master key 1601 is controlled as described above, and a generation number is correlated with each generation. The master key 1601 is a key used in common in a plurality of recording/playback devices, for example, a key common to devices 0 to 3 belonging to the dotted-line group shown in Fig. 11. A device ID is the identifier of the recording/playback device 1600 and is an identifier stored beforehand therein, such as a serial number in production. The device ID may be open to the public. The cognizant key 1631 and the non-cognizant key 1632 correspond to recording modes, respectively, and are common to a plurality of recording/playback devices. These keys are stored beforehand in the memory of the recording/playback device 1600.

[0181] The recording/playback device 1600 checks the recording medium 1620 as an optical disk about whether the disk ID 1603 as identification information has already been recorded. If the disk ID 1603 has been recorded, the recording/playback device 1600 reads the disk ID 1603 (Fig. 16). If the disk ID 1603 has not been recorded, a disk ID 1701 is generated randomly or by a predetermined method such as random number generation by a cryptosystem unit 150, and is recorded on the recording medium (Fig. 17). The disk ID 1603 can be stored in a lead-in area or the like since the disk needs to have one disk ID.

[0182] The recording/playback device 1600 generates a disk unique key 1602 by using the master key 1601, a stamper ID 1680 that is recorded as secret information readable from the disk only in a special reading method, and the disk ID 1603.

[0183] The following two methods shown in Fig. 19 can be used as specific methods for generating the disk unique key 1602 by using the master key 1601, the stamper ID 1680 as secret information, and the disk ID 1603. In one method (example 1), the master key 1601, the stamper ID 1680, and the disk ID 1603 are input to a hash function using a block encryption function, and the obtained result is used. In another method (example 2), data which is obtained by the bit concatenation of the master key 1601, the stamper ID 1680 as secret information, and the disk ID 1603 is input to hash function SHA-1 defined in Federal Information Standard Publication (FIPS PUB) 180-1, and from the resultant 160-bit output, a necessary data length is used as the disk unique key 1602.

[0184] As described above, the stamper ID 1680 is highly secret information recorded on the disk. Arithmetic processes, such as the reading of the stamper ID 1680, and the generation of the disk unique key 1602 by using the stamper ID 1680, are executed inside the cryptosystem unit 150 so that secrecy is maintained. In other words, the secret information read from the disk is securely protected in the cryptosystem unit 150.

[0185] In embodiments of the invention, secret information that can be read by only a special reading method is read by only an appropriate device, that is, a device capable of reading the secret information. Under secure protection, the secret information is used for the process of generating keys for encrypting contents in, for example, a cryptosystem unit which is mounted in an LSI and which performs the generation of a highly protected cryptographic key, so that the secret information is not stored in an externally readable memory. Accordingly, there is no possibility that the secret information leaks, and playback of abnormal contents can be effectively prevented.

[0186] As described above, secret information such as a stamper ID is written in a disk in a manner different from an ordinary data writing technique, and can be read in a technique different from ordinary data reading. The processes of writing and reading the secret information are described later.

[0187] In the recording/playback device 1600, the cryptosystem unit 150 (see Fig. 1 or 2) generates a title key 1604 as a unique key for each time of recording, randomly or by a predetermined method such as random number generation, and records the title key 1604 on the disk 1620.

[0188] After that, a flag 1633 that indicates which of a cognizant mode or a non-cognizant mode is set as a recording mode 1635, and the recording mode 1635 is recorded on the disk 1620.

[0189] Here, the cognizant mode and the non-cognizant mode are described below.

[0190] In each content, whether or not the content can be copied under what conditions is designated beforehand by a content provider. Accordingly, in network connection, the designated conditions should be correctly posted from a device to another device. In the DTCP system, a method using copy control information is used to solve this problem. Concerning copy control information, there are two types of transmission techniques in accordance with device performance.

[0191] "Encryption Mode Indicator (EMI)" is a mechanism in which the two upper Sy bits in a packet header are used to send copy control information. By using this mechanism, a receiver device can easily perform accessing, and a content can be securely sent because the value of the Encryption Mode Indicator acts on a key for encrypting the content.

[0192] The Encryption Mode Indicator is used to indicate the encryption mode of the packet, and the generation modes of content encryption and decryption keys

are designated. By disposing the Encryption Mode Indicator in an IEEE 1394 packet header, a receiver device is allowed to easily know the type of a mode for encryption of the content, for example, without extracting an embedded copy control information (described later) in an MPEG transport stream.

[0193] Fig. 20 shows an IEEE 1394 packet format. In "Data Field", various types of contents, such as music data and image data, are stored. The Encryption Mode Indicator (EMI) as copy control information is set as two upper Sy bits in a packet header.

[0194] The 2-bit EMI information defines a different type of treatment in accordance with the set value. Specifically, value "00" is "Copy Free" indicating that neither authentication nor encryption is not required and that a content may be freely copied. Value "01" is "Copy One Generation" indicating that 1-generation copying may be performed. Value "10" is "No More Copies" indicating that, after the above Copy One Generation is recorded once, recopying is inhibited. Value "11" is "Never Copy" indicating that the copying of a content is inhibited from the release thereof.

[0195] In the non-cognizant recording mode, in order that a bit stream recorder, such as D-VHS or hard disk, which does not recognize the format of data to be recorded may correctly treat copyrighted material, it is only necessary to update the Encryption Mode Indicator, without requiring the updating (e.g., Copy One Generation to No More Copies) the embedded copy control information when content recording is performed.

[0196] Conversely, in a format (e.g., DV-format) in which an area for sending copy control information is reserved, the copy control information can be sent as part of a content. Copy control information that is embedded as part of the content, as described above, is called "embedded copy control information". Normally, when a content is encrypted and transferred, embedded copy control information is similarly encrypted and transferred. It is considered that an intentional change of the embedded copy control information is difficult.

[0197] Here, in the case of a content having both the above 2-bit EMI copy control information and the embedded copy control information, a recording device that performs content recording updates the two types of copy control information, namely, both the Encryption Mode Indicator and the embedded copy control information. However, in the case of a recording device that does not have ability to analyze the embedded copy control information, the Encryption Mode Indicator is updated but the embedded copy control information is not updated.

[0198] A recording technique in which in a content recording mode, after updating embedded copy control information transmitted as part of a content, a recording device records the content with the updated embedded copy control information, is called a "cognizant mode". In comparison between the cognizant mode and the non-cognizant mode, the non-cognizant mode causes

a small load and can be easier employed because the updating of the embedded copy control information does not need to be performed. However, the DTCP has a rule in which in order that a device may perform MPEG decoding of a content and may output a video signal from an analog terminal, the device should employ the cognizant mode. Accordingly, a device having a decoding/display function should have a function of executing the cognizant mode.

[0199] In addition, in order to execute the cognizant mode, it is necessary to completely know the position and meaning of the embedded copy control information which is embedded as part of the content. For example, concerning a new or updated data format established after a certain device goes on the market, an old device may have a great difficulty in executing the cognizant mode in the new or updated data format.

[0200] Accordingly, it is possible that, for a specified data format or implementing a specified function, a content recording device execute the cognizant mode, while for recording a content having a different data format, the content recording device execute the non-cognizant mode.

[0201] There is a type of device that only performs recording using the non-cognizant mode for all contents. Conversely, there may be a type of device that only executes processing for contents having formats capable of understanding embedded copy control information, in other words, a type of device that only executes the cognizant mode.

[0202] As described above, in circumstances in which two type of copy control information, namely, Encryption Mode Indicator and embedded copy control information exist, and both a device that executes the cognizant mode and a device that executes the non-cognizant mode exist, it is preferable to distinguish between a content recorded in the cognizant mode and a communication network recorded in the non-cognizant mode.

[0203] In other words, when the cognizant mode is used to perform content recording, both types of copy control information, namely, Encryption Mode Indicator and embedded copy control information are updated, but when the non-cognizant mode is used to perform content recording, only Encryption Mode Indicator is updated and embedded copy control information is not updated. As a result, mismatching occurs between the Encryption Mode Indicator and the embedded copy control information recorded on a recording medium, and the mismatched Encryption Mode Indicator and embedded copy control information mix to cause confusion. That is why the distinction of the contents is preferable. Therefore, in order to prevent the two types of copy control information from being mismatched, for the content recorded in the cognizant mode, cognizant-mode recording/playback processing should be executed, and for the content recorded in the non-cognizant mode, non-cognizant-mode recording/playback processing should be executed.

[0204] Accordingly, one idea is that the cognizant mode and the non-cognizant mode are treated as separate recording modes. In this case, in order for a device to selectively execute both modes, the device should have processing configurations for executing both modes. This causes a problem in that the cost of the device is increased.

[0205] According to embodiments of the invention in accordance with either the cognizant mode or the non-cognizant mode, by generating a content-encryption key which is different from that used in the other mode, the two recording modes can be distinguished in accordance with the device and the recording mode used for recording the content, and a situation can be eliminated in which recording is performed with the two modes used in disorder. This implements a content processing configuration using either recording mode in accordance with the device and the recording mode used for recording the content, without increasing the configuration and processing load of the device.

[0206] Specifically, an encryption/decryption-key generating key (cognizant key) as secret information (necessary for playback) for cognizant-mode recording is provided and stored in only a device having a function of recording or playback using the cognizant mode, and an encryption/decryption-key generating key (non-cognizant key) as secret information (necessary for playback) for cognizant-mode recording is provided and stored in only a device having a function of recording or playback using the non-cognizant mode.

[0207] In this construction, concerning, for example, a content recorded using the cognizant mode, a device that has only a non-cognizant-mode recording/playback function can be prevented from executing, by a bug, manipulation of data, or unauthorized change of recording/playback program, mistaken or dishonest recording/playback.

[0208] Referring back to Figs. 16 and 17, the description of the content recording processing is continued.

[0209] The recording/playback device 1600 further acquires the generation number of the master key for use, namely, the generation number (generation #n) 1650 of the master key to be stored by itself, and stores the acquired generation number as a recording-mode generation number 1651 on the recording medium 1620.

[0210] On the recording medium 1620 as a disk, there is a data management file that stores information about which data forms which title. In the data management file, a title key 1605, the recording mode flag 1635, and the recording-mode generation number 1651 can be stored.

[0211] On the recording medium 1620, pre-recording-mode generation numbers are recorded beforehand. Only each content stored after being encrypted using a master key of a generation which is identical to a pre-recording-mode generation number or is newer than the pre-recording-mode generation number can be played

back. This construction is described in playback processing described later.

[0212] Next, among combinations, namely, a combination of a disk unique key and a title key, and combinations of a cognizant key or a disk unique key, the title key, and the non-cognizant key, any combination is used to generate a title unique key.

[0213] Specifically, when the recording mode is the cognizant mode, the disk unique key, the title key, and the cognizant key are used to generate the title unique key. When the recording mode is the non-cognizant mode, the disk unique key, the title key, and the non-cognizant key are used to the title unique key.

[0214] As described above, the encryption/decryption-key generating key (cognizant key) as secret information for cognizant-mode recording is stored in only the device having the function of recording or playback using the cognizant mode, while the encryption/decryption-key generating key (non-cognizant key) as secret information for cognizant-mode recording is stored in only the device having a function of recording or playback using the non-cognizant mode. Accordingly, in a device adapted for either recording mode, either recording mode is selected and content recording is executed. In other words, the use of the recording mode is limited to either the use of the cognizant key or the user of the non-cognizant key.

[0215] In the case of a device in which both keys are stored and both recording modes can be executed, a process is required which determines whether either recording mode should be executed. This mode determination process, that is, a process for determining whether the cognizant mode or the non-cognizant mode is used to perform content recording is described below with reference to Fig. 21.

[0216] Basically, it is preferable to perform content recording by the cognizant mode if possible. This is, as described above, because Encryption Mode Indicator and embedded copy control information are prevented from being mismatched. However, there is a possibility that a data analysis error, etc., occurs due to emergence of a new data format, etc., as described above. In such a case, recording using the non-cognizant mode is executed.

[0217] Each step in Fig. 21 is described below.

[0218] In step S5001, a recording device determines whether it can analyze a data format. As described above, embedded copy control information is embedded in a content, and impossibility of the data format analysis indicates that the reading of the copy control information is impossible. In this case, recording using the non-cognizant mode is executed.

[0219] When the data format analysis is possible, the recording device proceeds to step S5002, and determines whether it can perform data (content) decoding, the reading of embedded copy control information, and updating. The content and the embedded copy control information are normally encoded, so that the reading

of the embedded copy control information requires the execution of decoding. For example, in a case in which the device cannot perform decoding processing for the reason that a decoding circuit has already been used when multichannel simultaneous recording is performed, the embedded copy control information cannot be read, so that recording using the non-cognizant mode is executed.

[0220] In step S5002, if the recording device has determined that it can perform data (content) decoding, the reading of embedded copy control information, and updating, in step S5003, the recording device determines whether or not an input to the recording device by a user includes an input designating the execution of recording using the non-cognizant mode. Step S5003 is a step that is executed in only a device in which mode selection designated by the user can be performed, and is not executed in an ordinary device, that is, a device that does not allow the user to designate a mode. When the user inputs designation of the non-cognizant mode, recording using the non-cognizant mode is executed.

[0221] In step S5004, the recording device determines whether or not a content packet (e.g., received data) includes designation of executing recording using the non-cognizant mode. If the determination is affirmative, recording using the non-cognizant mode is executed. If the determination is negative, recording using the cognizant mode is executed.

[0222] In the device that can selectively execute recording using the cognizant mode and recording using the non-cognizant mode, the above-described mode determination process is used to determine the execution of recording using either mode. However it is understood from Fig. 21 that when recording using the cognizant mode is possible, recording using the cognizant mode is basically executed.

[0223] As described above, when the cognizant mode is used as the recording mode, the disk unique key, the title key, and the cognizant key are used to generate the title unique key, while when the non-cognizant mode is used the recording mode, the disk unique key, the title key, and the non-cognizant key are used to generate the title unique key.

[0224] Fig. 22 shows specific methods for generating the title unique key.

[0225] One method (example 1) uses a result obtained by inputting, to a hash function using a block encryption function, the title key, the disk unique key, and the cognizant key (in the case of the cognizant mode) or the non-cognizant key (in the case of the non-cognizant key).

[0226] In another method, after inputting, to hash function SHA-1 defined in FIPS PUB 180-1, data generated by the bit concatenation of the master key, the disk ID, and the cognizant key (in the case of the cognizant mode) or the non-cognizant key (in the case of the non-cognizant key), only a necessary data length in the resultant 160-bit output is used as the title unique

key.

[0227] In the above description, the master key, the stamper ID, and the disk ID are used to generate the disk unique key, and the disk unique key, and either the cognizant key or the non-cognizant key are used to generate each title unique key. However, without using the disk unique key, by using the master key, the disk ID, the title key, and either the cognizant key or the non-cognizant key, the title unique key may be directly generated. Also, without using the title key, by using the master key, the disk ID, and either the cognizant key or the non-cognizant key, a key corresponding to the title unique key may be generated.

[0228] By way of example, when one of transmission formats defined in the above DTCP is used, there is a case in which data is transmitted by TS packets in MPEG-2. For example, when a set-top box (STB) which receives a satellite broadcast uses the DTCP to transmit the broadcast to a recording device, it is preferable that the STB send MPEG-2 TS packets transmitted via the satellite broadcast link, also on the IEEE 1394 because data conversion does not need to be performed.

[0229] The recording/playback device 1600 receives content data to be recorded in the form of TS packets, and uses the TS processing unit 300 to add an arrival time stamp, which is information on the reception time of each TS packet. As described above, the block seed which is added to the block data may be formed by a combination of the arrival time stamp, the copy control information, and other information.

[0230] By arranging X (e.g., 32) ATS-added TS packets, one block of block data is formed (see the upper image in Fig. 5). As shown in Fig. 16 or 17, from a block seed having a 32-bit arrival time stamp, which is output by separating (selector 1608) the first to fourth bytes of the start of the block data input as data to be encrypted, and the already generated title unique key, a block key as a key for encrypting the data of the block data is generated (1607).

[0231] Fig. 23 shows two methods for generating the block key. In each method, from a 32-bit block seed and a 64-bit title unique key, a 64-bit block key is generated.

[0232] In the upper example 1, an encryption function is used which has a key length of 64 bits and an input/output length of 64 bits. A title unique key is used as a key for the encryption function, and a result that is obtained by inputting to the encryption function a concatenation value of a block seed and a 32-bit constant is used as a block key.

[0233] In the lower example 2, hash function SHA-1 defined in FIPS PUB 180-1 is used. Reduced data having 64 bits is used as a block key. For example, a concatenation value of a title unique key and a block seed is input to hash function SHA-1, and from the resultant 160-bit output, only lower-64-bit part is used.

[0234] Using Fig. 23, examples in which the disk unique key, the title unique key, and the block key are generated have been described. However, without ex-

executing the generation of the disk unique key and the title unique key, the block key may be generated by using, for each block, a master key, a stamper ID, a disk ID, a title key, a block seed, and a cognizant key (in the case of the cognizant mode) or a non-cognizant key (in the case of the non-cognizant mode).

[0235] After the block key is generated, the generated block key is used to encrypt block data. As the bottom of Figs. 16 and 17 shows, the initial first to m-th (e.g.,  $m = 8$ ) bytes of the block data including the block seed are separated (by a selector 1608) and are not encrypted. The (m+1)th byte to the final byte are encrypted (1609). The m bytes that are not encrypted include the first to fourth bytes as a block seed. The block data after the (m+1)th byte which is separated by the selector 1608 are encrypted (1609) in accordance with an encryption algorithm preset in the cryptosystem unit 150. For example, the Data Encryption Standard (DES) defined in FIPS 46-2 can be used as the encryption algorithm.

[0236] As described above, the block seed may include copy control information. Accordingly, when recording using the cognizant mode is executed, copy control information that corresponds to embedded copy control information, which is embedded in content data, is recorded. When recording using the non-cognizant mode is executed, copy control information that reflects the Encryption Mode Indicator (EMI) in the packet header in Fig. 20 is recorded.

[0237] In other words, in the case of information recording processing using the cognizant mode, record-information generating processing is executed in which a block seed including copy control information based on embedded copy control information in data part is added to a block data composed of at least one packet. In the case of information recording processing using the non-cognizant mode, record-information generating processing is executed in which a block seed including copy control information based on the Encryption Mode Indicator as copy control information included in a packet is added to a block data composed of at least one packet.

[0238] Here, when the block length (input/output data size) of an encryption algorithm for use is eight bytes as in the DES, by letting X be 32, and m be a multiple of 8, the entire block after the (m+1)-th byte can be encrypted without generating a fraction.

[0239] In other words, when assuming that the number of TS packets to be stored in one block is x, the input/output data size of the encryption algorithm is L bytes, and n is an arbitrary natural number, by determining X, m, and L so that  $192 * X = m + n * L$  can hold, the need for fraction processing is eliminated.

[0240] The encrypted block data after the (m+1)th byte is combined with the data of the first to m-th bytes by the selector 1610, and the combination is stored as encrypted content on the recording medium 1620.

[0241] In the above-described processing, in units of blocks, contents are encrypted using a block key gen-

erated based on a block seed including a generation-controlled master key and an arrival time stamp, and are stored on a recording medium.

[0242] As described above, according to embodiments of the invention content data is encrypted using a generation-controlled master key, and is recorded on a recording medium. Thus, for enabling decoding or playback, it is conditioned that playback processing on the recording medium is performed by a recording/playback device having the generation of a master key which is at least identical to or newer than the generation of a master key used for recording data.

[0243] As described above, in the case of recording using the cognizant mode, the block key is generated based on the cognizant key, while in the case of recording using the non-cognizant mode, the block key is generated based on the non-cognizant key. The data encrypted using the modes can be read only by a device having a key (the cognizant key or the non-cognizant key) corresponding to a mode identical to that used for recording.

[0244] In other words, the cognizant key is supplied only to a device that can recognize and update embedded copy control information which is embedded in a stream when performing recording and to a device allowed to read the data. A device that does not have the cognizant key cannot read a content recorded using the cognizant mode.

[0245] Similarly, the non-cognizant key is supplied only to a device having a non-cognizant recording mode that does not recognize embedded copy control information in a stream when recording is performed and to a device allowed to read data recorded in the mode. A device that does not have the non-cognizant key is designed so as not to a content recorded using the non-cognizant mode. Details of the playback processing are described later.

[0246] Next, with reference to the flowchart shown in Fig. 18, both the arrival-time-stamp adding processing by the TS processing unit 300 and the encryption processing by the cryptosystem unit 150, which are executed in accordance with data recording processing, are described below.

[0247] In step S1801, the recording/playback device reads a master key and the cognizant key or the non-cognizant key from the memory 180. The recording/playback device reads a stamper ID from a disk as a recording medium.

[0248] In step S1802, the recording/playback device determines whether a disk ID has already been recorded as identification information on the disk. If the determination is affirmative, in step S1803, the disk ID is read. If the determination is negative, in step S1804, the disk ID is generated randomly or by a predetermined method, and is recorded on the recording medium. In step S1805, a master key and a stamper ID are used to generate a disk unique key. The disk unique key is found by applying, for example, a method using hash function

SHA-1 defined in FIPS PUB 180-1, a method using a hash function based on block encryption, etc.

[0249] In step S1806, a title key is generated as a unique key for each time of recording, and is recorded on the disk, with the recording mode and the generation number of the master key. The recording mode represents a type of information recording mode, namely, either the cognizant mode or the non-cognizant mode.

[0250] In step S1807, a title unique key is generated by using the disk unique key, the title key, and the cognizant key (in the case of the cognizant mode) or the non-cognizant key (in the case of the non-cognizant mode).

[0251] Fig. 24 is a detailed flowchart showing the generation of the title unique key. In step S2001, the cryptosystem unit 150 proceeds to different steps depending on the recording mode. This branching is determined based on the program of the recording/playback device and designation data input by a user of the recording/playback device.

[0252] In step S2001, if the cryptosystem unit 150 has determined that the recording mode is the cognizant mode, it proceeds to step S2002, and generates the title unique key by using the disk unique key, the title key, and the cognizant key.

[0253] In step S2001, if the cryptosystem unit 150 has determined that the recording mode is the non-cognizant mode, it proceeds to step S2003, and generates the title unique key by using the disk unique key, the title key, and the non-cognizant key. The title unique key is generated by using a method using hash function SHA-1 defined in FIPS PUB 180-1, and a method using a hash function based on block encryption.

[0254] In step S1808, the recording/playback device receives, in the form of TS packets, data to be encrypted of content data to be recorded. In step S1809, the TS processing unit 300 adds each arrival time stamp (ATS) as information on a time at which each TS packet is received. Alternatively, the TS processing unit 300 adds each value obtained by combining copy control information, an arrival time stamp, and other information.

[0255] In step S1810, the recording/playback device sequentially receives the ATS-added TS packets, and determines whether the received packets has reached, for example,  $X = 32$  which forms one block, or whether it has received identification data indicating the end of the packets. If either condition is satisfied, the recording/playback device goes to step S1811, and forms one block of block data by arranging  $X$  ATS-added TS packets or ATS-added TS packets up to the end packet.

[0256] In step S1812, the cryptosystem unit 150 generates a block key as an encryption key for encrypting the block data by using the first 32 bits (the block seed including the arrival time stamp) and the title unique key generated in step S1807.

[0257] In step S1813, the generated block key is used to the block data formed in step S1811. As described above, the encryption range is the  $(m+1)$ th byte to the

end byte of the block data. The Data Encryption Standard defined in the FIPS 46-2 is applied to the encryption algorithm.

[0258] In step S1814, the encrypted block data is recorded on the recording medium. In step S1815, the recording/playback device determines whether all data have been recorded. If the determination is affirmative, the recording is terminated. If the determination is negative, the recording/playback device goes back to step S1808, and the remaining data is processed.

[0259] In accordance with the above process, the content recording processing is executed using the cognizant mode or the non-cognizant mode. When the content recording processing is executed by the cognizant mode, a key for use in content encryption is generated based on the cognizant key. When the content recording process is executed using the non-cognizant mode, a key for use in content encryption is generated based on the non-cognizant key. Accordingly, for the content recorded on the disk, it is required that a decryption key be generated by using either of the cognizant key and the non-cognizant key, or a single key. This can prevent recording and playback processing in which both modes are used.

#### Writing and Playback of Secret Information

[0260] Next, secret-information writing and reading processes are described below in which secret information, such as the stamper ID 1680 shown in Fig. 16 or 17, is written on the disk by using a manner different from an ordinary data-writing technique and in which the written secret information is allowed to be read only in the case of applying a manner different from an ordinary data-reading technique.

#### Generation of Secret Information By Signal Disturbance

[0261] First, a structure in which various types of information signals, such as the stamper ID 1680, are recorded after being disturbed using M-series signals is described below.

[0262] Fig. 25 shows the structure of a write-signal generating modulation circuit. The circuit shown in Fig. 25 writes secret information (such as the stamper ID 1680) modulated based on an FG signal which rises whenever a disk on which data is written rotates by a predetermined angle.

[0263] After generating, based on the FG signal, channel clocks CK which is synchronized with the rotation of the disk, a PLL circuit 1041 supplies the channel clocks CK to the components of the circuit.

[0264] A timing generator (TG) 1042 generates an initialization pulse signal SY for initializing M-series generating circuits 1045A to 1045D at predetermined intervals by counting the channel clocks CK. The timing generator 1042 also generates and outputs a synchronization pattern selection signal ST which is synchronized

with the initialization pulse signal SY.

**[0265]** Secret information, such as the stamper ID 1680, is input to the modulation circuit in Fig. 25 at a bit rate which is extremely smaller than that of the channel clocks CK. A synchronizing pattern generating circuit 1043 generates and outputs a predetermined synchronizing pattern DY based on the initialization pulse signal SY.

**[0266]** The M-series generating circuits 1045A to 1045D are initialized by the initialization pulse signal SY, and output M-series M1 to M4, respectively. The M-series signals M1 to M4 are strings of data which have randomly changing logical values and in which a possibility that logic "1" occurs and a possibility that logic "0" occurs are equal to each other. The M-series M1 to M4 signals do not have any mutual relationship.

**[0267]** Arithmetic circuits (indicated by "X" in Fig. 25) 1046A to 1046D are formed by exclusive OR circuits, and output the results of exclusive OR operations on the M-series signals M1 to M4 and the bits b0 to b3 of secret information such as a stamper ID and a disk ID. This causes the secret information to be disturbed by the M-series signals M1 to M4.

**[0268]** A random number generating circuit 1047 generates and outputs a 2-bit random number R (any value of 0, 1, 2, and 3) to a data selector 1048 in units of channel clocks CK. In response to the value of the random number R, the data selector 1048 selectively outputs the results of operations from the arithmetic circuits 1046A to 1046D. For example, when the random number R = 0, the output of the arithmetic circuit 1046A is selected. When the random number R = 1, the output of the arithmetic circuit 1046b is selected. When the random number R = 2, the output of the arithmetic circuit 1046C is selected. When the random number R = 3, the output of the arithmetic circuit 1046D is selected.

**[0269]** In the above construction, by performing decryption based on the M-series signals M1 to M4, the results of operations by the arithmetic circuits 1046A to 1046D are treated as a series and are further disturbed without being affected by other arithmetic operation results.

**[0270]** A data selector 1049 selectively outputs the initialization pulse signal SY which is output from the synchronizing pattern generating circuit 1043 based on the synchronization pattern selection signal ST, and the output of the data selector 1048. Accordingly, after the initialization pulse signal SY rises, and a synchronizing pattern (e.g., "11011") in a predetermined clock period (e.g., a 5-clock period) occurs, the data selector 1048 is controlled to perform outputting.

**[0271]** On the disk, in a predetermined secret information write area, the output of the modulation circuit in Fig. 25 is written. Even if the same secret information is input to the modulation circuit, the form of write data differs depending on the random number R. This makes it possible to perform writing of data that cannot be analyzed in ordinary reading processing.

**[0272]** Next, with reference to Fig. 26, the playback process on the secret information written in the above-described technique is described below.

**[0273]** Fig. 26 shows the structure of a decryption processor that plays back the secret information such as a stamper ID by decrypting a digital playback signal DX read from the disk. Based on the digital playback signal DX, a PLL circuit 1081 reproduces and outputs the channel clocks CK to the components of the decryption processor.

**[0274]** After detecting a synchronizing pattern by identifying the digital playback signal DX based on the channel clocks CK, a synchronization detection circuit 1082 reproduces the initialization pulse signal SY from the result of detection. Based on the initialization pulse signal SY and the channel clocks CK, M-series generating circuits 1083A to 1083D output the M-series signals M1 to M4 generated in the writing mode.

**[0275]** Multiplication circuits (indicated by "X" in Fig. 26) 1084A to 1084D multiply the M-series signals M1 to M4 by the digital playback signal DX, respectively, and output the products. In the multiplication circuits 1084A to 1084D, the polarity of the digital playback signal DX is inverted in accordance with the logical value of each of the M-series signals M1 to M4, whereby the multiplications are executed. The digital playback signal DX is played back only by decryption based on the M-series signals M1 to M4.

**[0276]** Integrating circuits (indicated by "Σ" in Fig. 26) 1085A to 1085D integrate, based on the initialization pulse signal SY, the products output by the multiplication circuits 1084A to 1084D, and output the integrated results in accordance with the logical values of bits b1 to b3 of the secret information (e.g., stamper ID). Determination circuits 1086A to 1086D perform binary identification based on the initialization pulse signal SY of the integrated results output by the integrating circuits 1085A to 1085D, whereby the values of bits b0 to b3 are reproduced and output.

**[0277]** As described above, the secret information is input, as a string of four parallel bits b0 to b3, to the modulation circuit (Fig. 25), and are recorded after being disturbed by the four M-series signals M1 to M4 and the random number R. Thus, it is difficult to read the recorded secret information in the ordinary reading processing. When playback is performed, the M-series signals M1 to M4 can be generated based on the synchronizing pattern DY, and the generated M-series signals M1 to M4 and the decryption of the read signal enable the secret information to be output.

**[0278]** A recording/playback device which reads a stamper ID written by the above-described recording technique and which generates a content-encryption key based on the stamper ID or the like has a secret information decrypting unit having the structure shown in Fig. 26.

# Recording Secret Information in Inner Circumferential Part of Disk

**[0279]** Next, concerning other secret-information writing and reading processes, a construction is described below in which secret information (such as a stamper ID) is written in an area of the disk different from a write area for music data, etc., and the written information is stably read.

**[0280]** The top part (A) of Fig. 27 is a perspective view of a disk containing secret information such as a stamper ID. The secret information is recorded four times on one track of the disk, so that the secret information can be played back, even if the disk is partly damaged. The secret information includes areas for a header, a stamper ID, etc., and an error correcting code. Each bit of bit patterns indicating the information is formed by a minute area unit having a dimension of 50  $\mu\text{m}$ , which is greatly longer than that of each bit of a data area recorded as user data. In each of the stamper ID area and the error correcting code area, a synchronizing pattern is formed in which among three minute areas, only the center area has a pattern formed by changing the optical property of the recording surface. The synchronizing pattern enables timing control in the playback mode.

**[0281]** The data of the information area and the error correcting code area is divided into two-bit parts. When two-bit data (b1, b0) is logic "00", the optical property of only the first minute area is changed, and the logic is converted to logic "1000" for recording, as shown in the part (D1) of Fig. 27. As shown in the part (D2) of Fig. 27, when two-bit data (b1, b0) is logic "01", logic "0100" is recorded. As shown in the part (D3) of Fig. 27, when two-bit data (b1, b0) is logic "10", logic "0010" is recorded. As shown in the part (D3) of Fig. 27, when two-bit data (b1, b0) is logic "11", logic "0001" is recorded. Accordingly, on the disk, the percentage of presence of optical-property-changed areas is 0.3 or less, so that in the inner circumferential part of the disk, data reading can be performed since focussing servo control based on sufficient reflected light can be performed.

**[0282]** Fig. 28 shows the structure of an decryption unit used for reading the secret information recorded in the inner circumferential part of the disk. A PLL circuit 1160 uses the digital playback signal DX to reproduce and output the channel clocks CK.

**[0283]** By determining the signal level of the digital playback signal DX based on the channel clocks CK, a synchronization detection circuit 1161 detects a synchronizing pattern and outputs an initialization pulse signal SY.

**[0284]** For the minute areas (parts (D1) to (D4) of Fig. 27) following the synchronizing pattern (part (C) of Fig. 27), a timing generator (TG) 1162 outputs, based on the initialization pulse signal SY, sampling pulse signals T1 to T4 which rise in the centers of the minute areas.

**[0285]** Flip-flops (FFs) 1163A to 1163D latch, based

on the sampling pulse signals T1 to T4, digital playback signals. Accordingly, the signal levels of playback signals which are obtained from the four minute areas assigned to the two-bit data (b1, b0) of the information areas and the error correcting code area are latched and retained in the flip-flops 1163A to 1163D.

**[0286]** By determining the magnitudes of the playback signal levels from the flip-flops 1163A to 1163D, the two-bit data (b1, b0) of the information areas and the error correcting code area are played back and output by a maximum detecting circuit 1164. A parallel/serial conversion circuit (PS) 1165 sequentially converts the two-bit data (b1, b0) into serial data and outputs the serial data.

**[0287]** A recording/playback device which reads the stamper ID written by the above-described recording technique and which generates a content-encryption key based on the stamper ID includes the decryption unit structure shown in Fig. 28.

**[0288]** As described above, by employing special secret-information writing and reading techniques different from those for contents, secret information such as a stamper ID is recorded on a disk, and the stamper ID is used as source data for keys for use in content encryption and decryption. Thus, if another processing key leaks, it is impossible to read the secret information, and a possibility of leak can be greatly reduced. This enables security-enhanced content protection.

**[0289]** This Specification describes a case in which the secret information required for writing and playback of specified information to be recorded on the disk is set as a stamper ID. However, the secret information is not limited to the stamper ID. It is possible that various types of identification data, such as IDs set for disks, and different content IDs set for contents, or encryption keys or the like, be set as secret information to be recorded on the disk. By applying these types of secret information, a content-encryption key is generated.

**[0290]** The above recording/playback device has a structure capable of selectively using a key for generating an encryption/decryption key for recording using the cognizant mode and a key for generating an encryption/decryption key for recording using the non-cognizant mode, as shown in Fig. 16 or 17. A recording/playback device that executes only one of the modes stores either key, that is, a cognizant key or a non-cognizant key, and generates, based on the stored key, a block key for content encryption and decryption. Block diagrams that show the process of generating a content-encryption key in each recording/playback device storing a single key are shown in Figs. 29 and 30.

**[0291]** Fig. 29 shows a recording/playback device having only a cognizant key. This recording/playback device generates, based on the cognizant key and key generating data, an encryption key and a decryption key which are used for data recording on a recording medium and data playback from the recording medium in order to execute content encryption and decryption.

[0292] Fig. 30 shows a recording/playback device having only a non-cognizant key. This recording/playback device generates, based on the non-cognizant key and key generating data, an encryption key and a decryption key which are used for data recording on a recording medium and data playback from the recording medium in order to execute content encryption and decryption.

[0293] In each recording/playback device storing a single type of key, data recording/playback can be executed only in either mode.

#### Content-Data Decryption and Playback Processing Using Generation-Controlled Master Key

[0294] Next, processing in which encrypted contents recorded as described above on the recording medium are decrypted and played back is described below using the block diagram shown in Fig. 31 and the flowcharts shown in Figs. 32 to 34.

[0295] Concerning the decryption and playback process, the process flow is described in accordance with the flowchart in Fig. 32, with reference to the block diagram in Fig. 31.

[0296] In Fig. 32, in step S2401, a recording/playback device 2300 (Fig. 31) reads a disk ID 2302, a pre-recording-mode generation number 2350, and a stamper ID 2380 from a disk 2320, and also reads a master key 2301, a cognizant key 2331 and/or a non-cognizant key 2332 from its memory. As is clear from the above description of the recording process, the disk ID 2303 is recorded on the disk 2320 beforehand, or if it is not recorded, the disk ID 2303 is a disk unique identifier in which the identifier is generated in the recording/playback device 2300 and is recorded on the disk 2320.

[0297] The pre-recording-mode generation number 2360 is generation information which is beforehand stored on the disk 2320 as a recording medium and which is unique to the disk 2320. By comparing the pre-recording-mode generation number 2360 and the generation of the master key 2301 which is obtained in data recording, that is, a recording-mode generation number 2350, determination of whether or not the playback process can be performed. The master key 2301 is a generation-controlled secret key which is stored in the memory of the recording/playback device 2300 in accordance with the flow in Fig. 14. The cognizant key and the non-cognizant key are secret keys common in system, which correspond to the cognizant mode and the non-cognizant mode, respectively.

[0298] In step S2402, the recording/playback device 2300 reads, from the disk 2320, a title key 2305 corresponding to data to be read, a (data) recording mode 2335, and the generation number of a master key used when recording data, that is, the recording-mode generation number 2350. In step S2403, the recording/playback device 2300 determines whether or not data to be read can be played back. The detailed flowchart of the

determination is shown in Fig. 33.

[0299] In Fig. 33, in step S2501, the recording/playback device 2300 determines whether or not the recording-mode generation number 2350 read in step S2402 is newer than the pre-generation number 2360 read in step S2401. If the recording/playback device 2300 has determined that the generation represented by the recording-mode generation number 2350 does not follow the generation represented by the pre-generation number 2360, in other words, when the generation represented by the recording-mode generation number 2350 is older than the generation represented by the pre-generation number 2360, the recording/playback device 2300 determines that playback is impossible. The recording/playback device 2300 skips over steps 2404 to S2409 and terminates the process without performing playback. Accordingly, when the contents recorded on the disk 2320 are encrypted based on the master key 2301 having a generation older than the generation represented by the pre-recording generation number 2360, a playback of the contents is not allowed and the playback is not performed.

[0300] Specifically, when an unauthorized conduct is detected, the above processing determines that the unauthorized conduct corresponds to a case in which data is encrypted based on an old master key by using an authorized recorder which is not supplied with a latest generation master key and the encrypted data is recorded, whereby the above processing prevents a recording medium containing the inappropriately recorded data from being played back. This can exclude the use of the unauthorized recorder.

[0301] In step S2501, if the recording/playback device 2300 has determined that the generation represented by the recording-mode generation number 2350 follows the generation represented by the pre-generation number 2360, in other words, when the generation represented by the recording-mode generation number 2350 is identical to or newer than the generation represented by the pre-generation number 2360, and the recorded contents are encrypted based on a master key whose generation follows the generation represented by the pre-generation number 2360, the recording/playback device 2300 goes to step S2502. In step S2502, after the recording/playback device 2300 acquires generation information on encryption master key C stored in its memory, it determines whether or not the generation of the encryption master key C is identical to/newer than the generation represented by the recording-mode generation number 2350 and determines by comparing both generations.

[0302] In step S2502, if the recording/playback device 2300 has determined that the generation of the encryption master key C does not follow the generation represented by the recording-mode generation number 2350, in other words, when the generation of the encryption master key C which is stored in the memory is older than the generation represented by the recording-mode gen-

eration number 2350, the recording/playback device 2300 determines that a playback is impossible, and terminates this processing without performing the playback process by skipping over steps S2404 to S2409.

[0303] Conversely, in step S2502, if the recording/playback device 2300 has determined that the generation of the encryption master key C follows the generation represented by the recording-mode generation number 2350, in other words, when the generation of the encryption master key C which is stored in the memory is identical to or newer than the generation represented by the recording-mode generation number 2350, the recording/playback device 2300 goes to step S2503. In step S2503, the recording/playback device 2300 determines whether or not it possesses a key corresponding to the recording mode, that is, a cognizant key or a non-cognizant key.

[0304] In step S2503, if the recording/playback device 2300 has determined that it possesses the cognizant key or the non-cognizant key, it determines that a playback is possible. If it does not possess the cognizant key or the non-cognizant key, it determines that the playback is impossible.

[0305] When the playback is possible, the recording/playback device 2300 goes to step S2404. In step S2404, the disk ID 2303, the master key 2301, and the stamper ID 2380 are used to generate (2302 in Fig. 31) a disk unique key. Methods of generating the disk unique key include the following two methods: in one method, after inputting, to hash function SHA-1 defined in the FIPS 180-1, data generated by bit concatenation of the a master key and a disk ID, only a necessary data length in the resultant 160-bit output is used as the disk unique key; and in another method, by inputting, to a hash function using a block encryption function, a master key and a disk ID, the obtained result is used. The master key being used here is one read in step S2402 in Fig. 32, which has the generation (time) represented by the recording-mode generation number. If the recording/playback device 2300 retains a master key having a newer generation, the above method is used to create a master key having the generation represented by the recording-mode generation number, and a disk unique key may be generated using the generated master key.

[0306] In step S2405, a title unique key is generated. A detailed flowchart for generating the title unique key is shown in Fig. 34. In step S2601, the cryptosystem unit 150 executes determination of a recording mode. This determination is executed based on the recording mode 2335 read from the disk 2320.

[0307] In step S2601, if the cryptosystem unit 150 has determined that the recording mode is the cognizant mode, it goes to step S2602, and generates the title unique key by using the disk unique key, the title key, and the cognizant key.

[0308] In step S2601, if the cryptosystem unit 150 has determined that the recording mode is the non-cognizant mode, it goes to step S2603, and generates the

title unique key by using the disk unique key, the title key, and the non-cognizant key. For generating the title unique key, a method using hash function SHA-1, and a hash function based on block encryption are used.

[0309] In the above description, by using a master key, a stamper ID, and a disk ID, the disk unique key is generated, and by using the generated disk unique key, and a cognizant key or a non-cognizant key, a title unique key is generated. However, without using the disk unique key, by using the master key, the stamper ID, the disk ID, the title key, and the cognizant key or the non-cognizant key, the title unique key may be directly generated. Also, without using the title key, by using the master key, the stamper ID, the disk ID, and the cognizant key or the non-cognizant key, a key corresponding to the title unique key may be generated.

[0310] In step S2406, block data is sequentially read from encrypted content 2312 recorded in encrypted form on the disk 2320. In step S2407, a selector 2310 separates first four bytes as a block seed from the block data. The block seed, and the title unique key generated in step S2405 are used to generate a block key.

[0311] For generating the block key, the above constructions in Figs. 23A and 23B can be applied. In other words, a technique can be applied in which by using a 32-bit block seed and a 64-bit title unique key, a 64-bit block key can be generated.

[0312] In the above description, each of the disk unique key, the title unique key, and the block key is generated. However, for example, without executing the generation of the disk unique key and the title unique key, the block key may be generated for each block by using the master key, the stamper ID, the disk ID, the title key, the block seed, and the cognizant key or the non-cognizant key.

[0313] After the block key is generated, in step S2408, the block data encrypted using the block key is decrypted (2309), and is output as decrypted data via a selector 2308. In the decrypted data, arrival time stamps are added to transport packets constituting a transport stream. In the above-described TS processing unit 300, stream processing based the arrival time stamps is executed. After that, data can be used in the form of, for example, displaying an image, and playing music.

[0314] As described above, contents recorded on a recording medium after being encrypted in units of blocks can be played back such that the contents are decryption-processed using a block key generated based on a block seed including a arrival time stamp.

[0315] After using the block key to decrypt the encrypted block data, in step S2409, the recording/playback device 2300 determines whether the reading of all data is completed. If all data have already been read, this process ends. If the determination is negative, the recording/playback device 2300 goes back to step S2406 and reads the remaining data.

[0316] The above recording/playback device 2300 has a structure capable of selectively using an encryp-

tion/decryption-key generating key (cognizant key) for the cognizant mode and an encryption/decryption-key generating key (non-cognizant key) for the non-cognizant mode, as shown in Fig. 31. As shown in Figs. 29 and 30, in a recording/playback device that stores only one of the keys, that is, the cognizant key or the non-cognizant key, only the recording mode corresponding to the stored key of either mode is executed, and a content-decrypting block key is generated based on the stored key.

#### Processing Configuration Using Media Key Effective Only in Recording Medium

[0317] In the above embodiment, an enabling key block is used to transmit a master key to each recording/playback device. The recording/playback device uses the master key to record and play back data.

[0318] A master key is a key that is effective in the entire record of data at the point thereof. A recording/playback device that has obtained a master key at a point is allowed to decrypt data recorded at the point and data recorded in system prior to the point. However, from the property of the master key in which it is effective in the entirety of the system, a defect occurs in that the exposure of the master key affects the entirety of the system.

[0319] By setting a key transmitted using an enabling key block of a recording medium so that it is used not as a master key effective in the entire system but as a media key effective in only the recording medium, the influence of exposure of the key can be suppressed. A method that using a media key instead of a master key is described below as a second embodiment of the present invention. Differences from the above first embodiment are described.

[0320] Similarly to Fig. 13, Fig. 35 shows that after device 0 generates updating node key  $K(t)00$  by using an enabling key block at a point  $t$  which is recorded on the recording medium, and leaf key  $K0000$  and node keys  $K000$  and  $K00$  which are stored in device 0, device 0 uses node key  $K(t)00$  to obtain updating media key  $K(t)_{media}$ . The obtained updating media key  $K(t)_{media}$  is used when performing data recording on the recording medium and playback of the data.

[0321] In Fig. 35, the pre-recording generation number is not essential because concerning the media key, there is no concept of old and new generations, differently from the master key.

[0322] When a recording medium is loaded into each recording/playback device for data recording or playback, the recording/playback device calculates media key  $K(t)_{media}$  for the recording medium in accordance with the flowchart shown in Fig. 36, and uses the updating media key  $K(t)_{media}$  to access the recording medium.

[0323] The reading of an enabling key block in step S2801 and the processing of the enabling key block in step S2802 (Fig. 36) are similar to steps S1403 and

S1404 in Fig. 14.

[0324] In step S2803, the recording/playback device reads, from the recording medium, code  $Enc(K(t)00, K(t)_{media})$  obtained by using node key  $K(t)00$  to encode media key  $K(t)_{media}$ . In step S2804, the recording/playback device obtains the media key by decrypting the read code. If the recording/playback device is revoked from a group in the tree structure shown in Fig. 11, the media key cannot be obtained and recording on the recording medium and playback cannot be performed.

[0325] Next, data recording on the recording medium is described. Concerning the media key, there is no concept of old and new generations, differently from the master key. Thus, determination in the first embodiment (Fig. 15) of whether or not recording can be performed by comparing the pre-recording generation information and the generation of the master key is not performed, and it is determined that recording is possible if the media key has been obtained in the above process. Specifically, this is shown in the flowchart shown in Fig. 37. In Fig. 37, in step S2901, the process determines whether the media key has already been obtained. If the media key has been obtained, a content recording process is executed in step S2902.

#### Data Recording Process Using Media Key Effective in Only Recording Medium

[0326] The content recording process is described below with the block diagrams shown in Figs. 38 and 39 and with the flowchart shown in Fig. 40.

[0327] In the second embodiment, an optical disk is used as an example of a recording medium, similarly to the first embodiment. The first embodiment is also similar to the second embodiment in that in order that data on the recording medium may be prevented from being copied, a disk ID as identification information unique to the recording medium influences a data encrypting key.

[0328] Figs. 38 and 39 correspond to Figs. 16 and 17 in the first embodiment, and differ in that a media key is used instead of the master key and in that a recording-mode generation number that represents a master key generation is not used. Fig. 38 differs from Fig. 39 in that the writing of the disk ID is executed, similarly to the difference between Fig. 16 and Fig. 17.

[0329] Fig. 40 shows the data recording process of the second embodiment which uses the media key. The flowchart in Fig. 40 corresponds to that in Fig. 18 (the first embodiment). The flowchart in Fig. 40 is described below, mainly concerning differences from the first embodiment.

[0330] In Fig. 40, in step S3201, a recording/playback device 3000 reads a cognizant key and/or a non-cognizant key which are stored in its memory, and the media key  $K(t)_{media}$  temporarily stored after being calculated in step S2804 in Fig. 36. The recording/playback device 300 also reads a stamper ID from the disk.

[0331] In step S3203, the recording/playback device

3000 determines whether or not a disk ID has already been recorded as identification information on the recording medium (optical disk). If the disk ID has already been recorded, in step S3203, the recording/playback device 300 reads the disk ID (in the case of Fig. 38). If the disk ID has not already been recorded, in step S3204, a disk ID is generated by using a predetermined manner and is recorded on the disk (in the case of Fig. 39). The disk ID can be stored in a lead-in area or the like because the disk needs to have one disk ID. In either case, the recording/playback device 3000 goes to step S3205.

[0332] In step S3205, the media key and the stamper ID which are read in step S3201 are used to generate a disk unique key. A specific method of generating the disk unique key is identical to that used in the first embodiment, and the media key may be used instead of the master key.

[0333] In step S3206, a key that is unique to each time of recording, namely, a title key is generated randomly or by a predetermined method, and is recorded on the disk. Simultaneously, a recording mode activated when recording the title (data) is recorded on the disk.

[0334] The disk contains a data management file storing information that which data forms which title. The title key and the recording mode can be stored in the data management file.

[0335] A description of steps S3207 to S3215 is omitted since they are similar to steps S1807 to S1815 in Fig. 18.

[0336] In the above description, a disk unique key is generated by using a media key, a stamper ID, and a disk ID, and a title unique key is generated by using the disk unique key, a title key, a cognizant key or a non-cognizant key. However, without using the disk unique key, by using the media key, the stamper ID, the disk ID, the title key, and the cognizant key or the non-cognizant key, the title unique key may be directly generated. Also, without using the title key, by using the stamper ID, the disk ID, and the cognizant key or the non-cognizant key, a key corresponding to the title unique key may be generated.

[0337] As described above, data can be recorded on the recording medium by using the media key.

#### Data Playback Process Using Media Key Effective in Only Recording Medium

[0338] A process for playing back the data recorded as described above is described below with reference to the block diagram shown in Fig. 41 and the flowchart shown in Fig. 42.

[0339] Fig. 41 corresponds to Fig. 31 in the first embodiment, and differs in that since a media key is used instead of the master key, a recording-mode generation number is omitted.

[0340] In Fig. 42, in step S3401, a recording/playback device 3400 reads a stamper ID and a disk ID from a

disk 3420 as a recording medium, and also reads a cognizant key and/or a non-cognizant key and the media key temporarily stored after being calculated in step S2804 in step S36.

[0341] When the media key cannot be obtained by performing the process shown in Fig. 36 after loading the recording medium, the playback process is not performed and terminated.

[0342] In step S3402, the title key of data to be read from the disk 3320, and a recording mode stored when recording the data are read.

[0343] In step S3403, the recording/playback device 3300 determines whether or not the data can be played back. The details of step S3403 are shown in Fig. 43.

[0344] In step S3501, the recording/playback device 3300 determines whether or not the media key is obtained. If the media key is not obtained, a playback is impossible. If the media key is obtained, the recording/playback device 3300 goes to step S3502. Step S3502 is similar to step S2503 in Fig. 33. When the recording/playback device 3300 possesses a key corresponding to a recording mode used when recording the data (a cognizant key for the cognizant mode or a non-cognizant key for the non-cognizant mode), the recording/playback device 3300 determines that a playback is possible, and goes to step S3404. When the recording/playback device 3300 possesses the key, it determines that a playback is impossible, and skips over steps S3404 to S3409 and terminates the process without performing the playback.

[0345] A description of steps S3404 to S3409 is omitted since they are similar to steps S2404 to S2409 in Fig. 32.

[0346] In the above description, by using a media key, a stamper ID, and a disk ID, a disk unique key is generated, and by using the disk unique key, a title key, a cognizant key or a non-cognizant key, a title unique key is generated. However, without using the disk unique key, by using the media key, the stamper ID, the disk ID, the title key, and the cognizant key or the non-cognizant key, the title unique key may be directly generated. Also, without using the title key, by using the media key, the stamper ID, the disk ID, and the cognizant key or the non-cognizant key, a key corresponding to the title unique key may be generated.

[0347] As described above, data recording on the recording medium and the playback from the recording medium are executed.

#### Copy Control in Recording Process

[0348] To protect advantages of a content copyrighter, content copying should be controlled in a licensed device.

[0349] Specifically, when a content is recorded on a recording medium, it is required that after determining whether the content may be copied, only a content allowed to be copied be recorded. When a content record-

ed on the recording medium is played back and output. It is required that unauthorized copying of the output content be prevented.

[0350] Accordingly, processing by the recording/playback device 100 or 200 in Fig. 1 or 2 in a case in which content recording and playback is performed while performing the content copy control is described below with reference to the flowcharts shown in Figs. 44A to 45B.

[0351] When a digital signal content from the exterior is recorded on the recording medium, the recording process shown in Fig. 44A is performed. This recording process is described using the recording/playback device 100 shown in Fig. 1 as an example. When a digital signal content (digital content) is supplied to the input/output I/F 120 via, for example, an IEEE 1394 serial bus, in step S4001, the input/output I/F 120 receives the digital content and goes to step S4002.

[0352] In step S4002, the input/output I/F 120 determines whether the received digital content may be copied. Specifically, when the content received by the input/output I/F 120 is not encrypted, for example, when a plaintext content is supplied to the input/output I/F 120 without using the above-described DTCP, the input/output I/F 120 determines that the received content may be copied.

[0353] It is assumed that the recording/playback device 100 is a device based on the DTCP which executes the process in accordance with the DTCP. The DTCP defines 2-bit Encryption Mode Indicator as copy control information for controlling copying. When the Encryption Mode Indicator is "00B" where B indicates that the adjacent value is a binary number, the content is of "Copy-freely" type. When the Encryption Mode Indicator is "01B", the content is of a "No-more-copies" type in which the content may not be more copied. When the Encryption Mode Indicator is "10B", the content is "Copy-one-generation" type in which the copying of the content can be performed once. When the Encryption Mode Indicator is "11B", the content is "Copy-never" type in which copying of the content is inhibited.

[0354] When the signal supplied to the input/output I/F 120 in the recording/playback device 100 includes an Encryption Mode Indicator, and the Encryption Mode Indicator is of a type among Copy-freely and Copy-one-generation types, the input/output I/F 120 determines that the content may be copied. When the Encryption Mode Indicator is of a type among No-more-copies and Copy-never types, the input/output I/F 120 determines that the content is not allowed to be copied.

[0355] In step S4002, if the input/output I/F 120 has determined that the content may not be copied, steps S4003 to S4005 are skipped over and the recording process is terminated. Accordingly, in this case, the content is not recorded on the recording medium 195.

[0356] In step S4002, if the input/output I/F 120 has determined that the content may be copied, the process goes to step S4003. After that, steps S4003, S4004, and S4005 are performed which are similar to steps S302,

S303, and S304 shown in Fig. 3B. In other words, the addition by the TS processing unit 300 of the arrival time stamp to the transport packet, and encryption processing by the cryptosystem unit 150 are executed. The resultant encrypted content is recorded on the recording medium 195, and the recording process is terminated.

[0357] The Encryption Mode Indicator is included in the digital signal supplied to the input/output I/F 120, so that when the digital content is recorded, an Encryption Mode Indicator or information (e.g., embedded copy control information in the DTCP, etc.) which represents a copy-control status similarly to the Encryption Mode Indicator are also recorded, with the digital content.

[0358] In the recording, in general, information which represents Copy-One-Generation type is recorded after being converted into information which represents No-more-copies type so that more copies are not allowed.

[0359] In a recording/playback device of an embodiment of the invention, copy control information, such as Encryption Mode Indicator and embedded copy control information, is recorded in a form in which it is added to the TS packet. In other words, 32 bits which include an arrival time stamp having 24 to 30 bits and copy control information, as shown in examples 2 and 3 of Fig. 10, are added to each transport stream (TS) packet, as shown in Fig. 5.

[0360] When an analog signal content from the exterior is recorded on the recording medium 195, the recording process shown in Fig. 44B is performed, which is described below.

[0361] When the analog signal content is supplied to the input/output I/F 140, the input/output I/F 140 receives the analog signal content in step S4011 and goes to step S4012. In step S4012, the analog signal content determines whether the received analog signal content may be copied.

[0362] The determination in step S4012 is performed by, for example, determining whether or not the signal received by the input/output I/F 140 includes a Macrovision signal or a CGMS-A (Copy Generation Management System-Analog) signal. The Macrovision signal is a signal that becomes noise after being recorded on a VHS videocassette tape. When this is included in the signal received by the input/output I/F 140, the input/output I/F 140 determines that the analog content is not allowed to be copied.

[0363] The CGMS-A signal is such that a CGMS signal for use in digital signal copy control is applied to analog signal copy control. The CGMS-A signal represents one of Copy-freely type in which the content is allowed to be freely copied, Copy-one-generation type in which the copying of the content can be performed only once, and Copy-never type in which copying of the content is inhibited.

[0364] Accordingly, when the CGMS-A signal is included in the signal received by the input/output I/F 140 and represents one of the Copy-freely type and the Copy-one-generation type, it is determined that the an-

alog content may be copied. The CGMS-A signal represents the Copy-never type, it is determined that the analog content is not allowed to be copied.

[0365] In addition, for example, when the Macrovision signal and the CGMS-A signal are not included in the received by the input/output I/F 140, it is determined that the analog content may be copied.

[0366] In step S4012, if the input/output I/F 140 has determined that the analog content is not allowed to be copied, it skips over steps S4013 to S4017 and terminates the recording process. Accordingly, in this case, the content is not recorded on the recording medium 195.

[0367] In step S4012, if the input/output I/F 140 has determined that the analog content may be copied, it goes to step S4013. After that, steps S4013 to S4017 are performed which are similar to steps S322 to S326 shown in Fig. 3B, whereby after performing MPEG encoding, TS processing, and encryption processing, the content is recorded on the recording medium 195 and the recording ends.

[0368] When the analog signal received by the input/output I/F 140 includes the CGMS-A signal, and the analog content is recorded on the recording medium 195, the CGMS-A signal is also recorded. The CGMS-A signal is recorded in the copy control information or the other information shown in Fig. 10. In the recording, in general, information which represents Copy-One-Generation type is recorded after being converted into information which represents No-more-copies type so that more copies are not allowed. Although in the system, copy control information such as the Copy-one-generation type is recorded without being converted into the No-more-copies type, this does not apply to a case in which there is a rule that the copy control information is treated as the No-more-copies type.

#### Copy Control in Playback Process

[0369] Next, in a case in which the content recorded on the recording medium 195 is played back and output as a digital content to the exterior, the playback process shown in Fig. 45A is performed, which is described below.

[0370] First, steps S4101, S4102, and S4103 are performed which are similar to steps S401, S402, and S403, whereby the encrypted content read from the recording medium 195 is decrypted in the cryptosystem unit 150 and is processed by transport stream processing. The processed digital content is supplied to the input/output I/F 120 via the bus 110.

[0371] In step S4104, the input/output I/F 120 determines whether or not the supplied digital content may not be copied later. In other words, when the digital content supplied to the input/output I/F 120 does not include an Encryption Mode Indicator or information (copy control information) representing a copy control status, it is determined that the content may not be copied later.

[0372] When the digital content supplied to the input/output I/F 120 includes copy control information such as Encryption Mode Indicator, accordingly, when copy control information such as Encryption Mode Indicator is recorded in accordance with the DTCP in content recording, the recorded copy control information (recorded Encryption Mode Indicator) is of Copy-freely type, it is determined that the content may not be copied later. When copy control information such as Encryption Mode Indicator is of No-more-copies type, it is determined that the content is not allowed to be later copied.

[0373] In general, there is no case in which the recorded copy control information (Encryption Mode Indicator) is of Copy-one-generation type or Copy-never type. This is because the Copy-one-generation type of Encryption Mode Indicator is converted to No-more-copies type of Encryption Mode Indicator when performing recording and because a digital content having Copy-never type of Encryption Mode Indicator is not recorded on a recording medium.

[0374] In step S4104, if the input/output I/F 120 has determined that the digital content may not be copied later, it goes to step S4105, and outputs the digital content to the exterior. After that, the playback process ends.

[0375] In step S4104, if the input/output I/F 120 has determined that the digital content may not be copied later, it goes to step S4106. In step S4106, the input/output I/F 120 outputs the digital content to the exterior in accordance with the DTCP so that the digital content cannot be later copied. After that, the playback process ends.

[0376] In other words, when the recorded copy control information (Encryption Mode Indicator) is of No-more-memories type, or in a case in which the system has a rule that Copy-one-generation type of copy control information is recorded without being converted into No-more-memories type of copy control information, and copy control information (Encryption Mode Indicator) recorded under the rule is of Copy-one-generation type, the content may not be more copied.

[0377] Accordingly, the input/output I/F 120 performs mutual authentication with another device in accordance with the DTCP standard. When the device is right (or is based on the DTCP standard), the digital content is encrypted and output to the exterior.

[0378] Next, in a case in which the content recorded on the recording medium is played back and output as an analog content to the exterior, the playback process shown in Fig. 45B is performed, which is described below.

[0379] Steps S4111 to S4115 are performed which are similar to steps S421 to S425 shown in Fig. 4B. In other words, the reading of the encrypted content, transport stream processing, MPEG decoding, and D/A conversion are executed. The obtained analog content is received by the input/output I/F 140.

[0380] In step S4116, the input/output I/F 140 deter-

mines whether or not the supplied content may be copied. If copy control information such as Encryption Mode Indicator is not recorded with the content, the input/output I/F 140 determines that the content may be copied.

[0381] In a case in which when recording the content, copy control information such as Encryption Mode Indicator is recorded in accordance with the DTCP, and the copy control information is of Copy-freely type, the input/output I/F 140 determines that the content may not be copied later.

[0382] When the copy control information is of No-more-copies type, or when in the system there is, for example, a rule that Copy-one-generation type of copy control information is recorded without being converted and is treated as No-more-copies type of copy control information, and copy control information recorded under the condition is of Copy-one-generation type, the input/output I/F 140 determines that the content may not be copied later.

[0383] When the analog content supplied to the input/output I/F 140 includes, for example, a CGMS-A signal, in other words, in a case in which when recording the content, the CGMS-A signal is recorded with the content, and the CGMS-A signal represents Copy-freely type, it is determined that the analog content may not be copied later. If the CGMS-A signal represents Copy-never type, it is determined that the analog content may not be copied later.

[0384] In step S4116, if the input/output I/F 140 has determined that the analog content may not be copied later, it goes to step S4117. In step S4117, the input/output I/F 140 outputs the supplied analog signal to the exterior and terminates the playback process.

[0385] In step S4116, if the input/output I/F 140 has determined that the content may not be copied later, it goes to step S4118. In step S4118, the input/output I/F 140 outputs the analog content to the exterior in a form in which the analog content cannot be later copied, and the playback process ends.

[0386] For example, when the recorded copy control information is of No-more-copies type, as described above, or in a case in which in the system there is a rule that Copy-one-generation type of copy control information is recorded without being converted and is treated as No-more-copies type, and copy control information recorded under the condition is Copy-one-generation type, the content may not be more copied.

[0387] Therefore, after adding, for example, a Macrovision signal or a CGMS-A signal representing Copy-never type to the analog content, the input/output I/F 140 outputs the obtained content to the exterior. Also when the recorded CGMS-A signal represents Copy-never type, the content may not be more copied. Accordingly, after changing the CGMS-A signal to represent Copy-never type, the input/output I/F 140 outputs the changed CGMS-A signal to the exterior, with the analog content.

[0388] As described above, by recording or playing back a content while performing content-copy control,

copying (unauthorized copying) beyond the allowable range of the content can be prevented.

#### Structure of Data Processing Unit

[0389] The above successive processes can be performed not only by hardware but also by software. For example, although the cryptosystem unit 150 can be formed by an encryption/decryption LSI, processing by the cryptosystem unit 150 can be executed such that a general-purpose computer or a single-chip microcomputer executes programs. Similarly, processing by the TS processing unit 300 can be also performed by software. When software is used to perform successive processes, programs constituting the software are installed in a device such as a general-purpose computer or a single-chip microcomputer. Fig. 46 shows an example of a computer in which programs for executing the successive processes are installed.

[0390] The programs can be recorded beforehand on a hard disk 4205 or a read-only memory (ROM) 4203 as a recording medium which is built into the computer. Alternatively, the programs can be temporarily or eternally stored (recorded) in a removable recording medium 4210 such as a floppy disk, a CD-ROM, a magneto-optical disk, a digital versatile disk, a magnetic disk, or a semiconductor memory. The removable recording medium 4210 can be provided in the form of so-called "package software".

[0391] In addition to the installation of the programs from the removal recording medium 4210 in the computer, after transmitting the programs from a download site to the computer by radio via a satellite for digital satellite broadcasting or by wire via a network such as the Internet, the transmitted programs are received in a communication unit 4208 and can be installed in the hard disk 4205 in the computer.

[0392] The computer includes a CPU 4202. An input/output interface 4211 is connected to the CPU 4202 via a bus 4201. When a command is input by a user operating an input unit 4207 having a keyboard and a mouse, the CPU 4202 executes a program stored in a ROM 4203 in accordance with the input command.

[0393] Also, the program stored in the hard disk 4205, the program installed in the hard disk 4205 after being transmitted via a satellite or a network and received by the communication unit 4208, or the program installed in the hard disk 4205 after being read from the removal recording medium 4210 is loaded and executed in the CPU 4202.

[0394] This allows the CPU 4202 to perform the above processes in accordance with the above flowcharts or the processes performed by the block diagrams. The CPU 4202 outputs the obtained results from an output unit 4206 having a liquid crystal display, a speaker, etc., transmits them from the communication unit 4208, and records them on the hard disk 4205, as required.

[0395] Here, in this Specification, processing steps

that describe each program for controlling the computer to perform various types of processing do not always need to be time-sequentially performed along the order in flowchart form, and include processes (e.g., parallel processes or object-based processes) which are executed in parallel or separately.

[0396] Each program may be executed either by a single computer or by a plurality of computers. Each program may be executed after being transferred to a remote computer.

[0397] In the second embodiment a case in which a content encryption/decryption block is formed by a single-chip encryption/decryption LSI has been mainly described. However, the content encryption/decryption block can be implemented as a software module executed by the CPU 170 in Fig. 1 or 2. Similarly, also processing by the TS processing unit 300 can be implemented as a software module executed by the CPU 170.

#### Apparatus and Method for Producing Recording Medium

[0398] Next, an apparatus and method according to an illustrative embodiment of the invention that produce the above information recording medium are described below.

[0399] Fig. 47 shows a schematic structure of a disk production apparatus 4300 which produces a recording medium 4350 and records a disk ID, an enabling key block, and an encrypted master key or an encrypted media key on a recording medium.

[0400] In the disk production apparatus 4300, a disk ID, an enabling key block, and an encrypted master key or an encrypted media key are recorded on a recording medium 4350 which has already been assembled, with the above-described secret information. Also, pre-recording generation information of the master key is recorded, as required.

[0401] The disk production apparatus 4300 includes a memory 4302, or another storage unit, which contains disk IDs, enabling key blocks, and encrypted master keys or encrypted media keys, a recording medium I/F 4303 that performs reading/writing from/to the recording medium 4350, an input/output I/F 4304 as an interface with another apparatus, a control unit 4301 for controlling the above units, and a bus 4305 for establishing connection.

[0402] Although Fig. 47 shows the structure in which the memory 4302 and the recording medium I/F 4304 are included in the disk production apparatus 4300, they may be externally provided.

[0403] The disk ID, the enabling key block, and the encrypted master key or the encrypted media key, the secret information such as stamper ID, and the pre-recording generation information of master key are issued by an identifier management department, a key issuing center, etc., which are not shown, and are stored beforehand in the internal or external memory 4302.

[0404] The disk ID, the enabling key block, and the encrypted master key or the encrypted media key, the secret information, the pre-recording generation information of master key, which are stored in the memory 4302, are recorded on the recording medium 4350 via the recording medium I/F 4303 under control of the control unit 4301. The pre-recording generation information of master key is also recorded, as required.

[0405] The secret information is data generated by a secret information generator having the construction described in the Writing and Playback of Secret Information section, which are shown in, for example, Figs. 25 and 27. In accordance with the controller, data conversion of the secret information is performed, and the resultant converted data is written on the recording medium 4350.

[0406] Concerning the disk ID, the enabling key block, and the encrypted master key or the encrypted media key, the secret information such as stamper ID, and the pre-recording generation information of master key, not only those stored in the memory 4302, but also those sent from the key issuing center via the input/output I/F 4304 can be used.

[0407] Fig. 48 shows a production flow in a recording medium production method according to an embodiment of the invention in which in the production of a recording medium, the disk ID, the enabling key block, and the encrypted master key or the encrypted media key, the secret information, and the pre-recording generation information of master key are recorded on a recording medium.

[0408] Referring to Fig. 48, in step S4401, a known assembly process (not shown) is used to assemble a recording medium such as a DVD or a Cited document.

[0409] In step S4402, the recording medium production apparatus shown in Fig. 47 executes processing of recording, on the assembled recording medium, a disk ID, a stamper ID as secret information, an enabling key block, and an encrypted master key or an encrypted media key. Pre-recording generation information is also recorded, as required.

[0410] By using the above disk production process, the recording medium is shipped from a production factory in the form of containing the disk ID, the stamper ID as secret information, the enabling key block, the encrypted master key or the encrypted media key. Also, the recording medium is shipped from the production factory after the pre-recording generation number is recorded on the recording medium, as required.

[0411] The recorded secret information is not limited to the stamper ID. A disk ID set for each disk, a content ID for each content, a cryptographic key, various types of identification data, and an encryption key may be recorded as the secret information. A recording/playback device of an embodiment of the invention uses the various types of secret information to generate a content-encryption key.

# Format of Enabling Key Block

[0412] Fig. 49 shows an example of a format of the enabling key block. In Fig. 49, a version 4501 is an identifier indicating the version of an enabling key block. A depth 4502 indicates a hierarchical-tree level number of a device to which the enabling key block is distributed. A data pointer 4503 indicates the position of a data part in the enabling key block. A tag pointer 4504 indicates the position of a tag part in the enabling key block. A signature 4508 indicates the position of a signature in the enabling key block. A data part 4506 stores, for example, data generated by encrypting a node key to be updated.

[0413] The tag part 4507 indicates the positional relationship of the encrypted node keys and leaf key which are stored in the data part 4506. A rule of providing the tag is described with reference to Fig. 50. Fig. 50 shows an example of sending, as data, the enabling key block described using Fig. 12A. The data is as shown in the table of the right portion (b) of Fig. 50. The address of a top node included in an encryption key in this case is used as a top node address. As shown in the table, the top node address is KR because updating key K(t)R of root key is included.

[0414] Top encryption-key data Enc(K(t)0, K(t)R) corresponds to a denoted position in the hierarchical tree of the left portion (a) of Fig. 50. Next data is represented by Enc(K(t)0, K(t)0) and corresponds to a lower left position from the previous data. The presence of data is indicated by a tag value of "0", while the absence of data is indicated by a tag value of "1". Each tag is set as {left (L) tag, right (R) tag}. Since the left of top encryption-key data Enc(K(t)0, K(t)R) has data, L tag = 0. Since the right of top encryption-key data Enc(K(t)0, K(t)R) has no data, R tag = 1. Tags are set for all of data, so that a data string and a tag string are formed, as shown in the bottom portion (c) of Fig. 50.

[0415] Concerning the order of node processing in the tree, it is preferable to use one of breadth first processing in which widthwise processing at the same level is first performed, and depth first processing in which depthwise processing is first performed.

[0416] Referring back to Fig. 49, the format of the enabling key block is further described below.

[0417] The signature is a digital signature performed by an authority that issues the enabling key block, such as key-management center, content provider, settlement authority. A device that receives the enabling key block uses signature verification to verify that the received enabling key block is issued by a right enabling key block issuer.

[0418] In so far as the embodiments of the invention described above are implemented, at least in part, using software-controlled data processing apparatus, it will be appreciated that a computer program providing such software control and a transmission, storage or other medium by which such a computer program is provided

are envisaged as aspects of the present invention.

[0419] With reference to specified embodiments, the present invention has been described. However, it is obvious that a person skilled in the art will make a modification or substitution of the embodiments without departing from the scope of the present invention. For example, as described above, the foregoing embodiments describe a case in which a stamper ID is used as the secret information required for writing of data to be stored on a disk and playback processing.

[0420] However, the secret information is not limited to the stamper ID, but may be a disk ID differently set for each disk, a content ID set for each content, a cryptosystem key, various identification data, and an encryption key. In the foregoing embodiments, the present invention has been exemplified and should not be limitedly interpreted.

## Claims

1. An information recording device for recording information on a recording medium, comprising:

cryptosystem means for executing encryption processing on data to be stored on said recording medium; and  
secret-information decoding means for reading secret information stored on said recording medium by executing a special data-reading process which is different from a process of reading content data stored on said recording medium;

wherein said cryptosystem means generates a content-encryption key by using, as a key-generating data, the secret information which is decoded after being read from said recording medium, and executes, based on the content-encryption key, the encryption processing on the data to be stored.

2. An information recording device according to Claim 1, wherein:

the secret information includes a type of data among a stamper ID which is stored on said recording medium when said recording medium is produced and which is common to a plurality of recording media, a disk ID which is unique to each of the recording media, a content ID which is differently set for each content, and a cryptosystem key; and  
said secret-information decoding means executes a decoding process on the read data.

3. An information recording device according to Claim 1, wherein said cryptosystem means uses the read secret information to generate the content-encryption key, and the read secret information is allowed

to be used only in the generation of the content-encryption key which is executed in said cryptosystem means, without being stored in storage means which is readable from the outside of said information recording device.

4. An information recording device according to Claim 1, wherein:

said information recording device possesses node keys which are unique to nodes constituting a hierarchical tree structure having a plurality of different information recording devices as leaves;  
said cryptosystem means generates the content-encryption key based on the read secret information and encryption-key-generating data which is stored in said information recording device; and  
the encryption-key-generating data can be updated by using an enabling key block generated such that a node key is encrypted by using a key including at least one of a node key and a leaf key which are positioned at a lower level.

5. An information recording device according to Claim 4, wherein the encryption-key-generating data is one of a master key common to a plurality of information recording devices and a media key unique to a specified recording medium.

6. An information recording device according to Claim 4, wherein:

the encryption-key-generating data corresponds to a generation number as updating information; and  
when storing encrypted data on said recording medium, said cryptosystem means stores on said recording medium the generation number of the encryption-key-generating data as a recording-mode generation number.

7. An information recording device according to Claim 4, further comprising transport-stream processing means for adding an arrival time stamp to each of transport packets constituting a transport stream;

said cryptosystem means generates a block key as an encrypted key for block data composed of at least one transport packet to which the arrival time stamp is added; and  
in encryption of the data to be stored on said recording medium, said cryptosystem means generates a block key as an encryption key based on data including the secret information, the encryption-key-generating data, and a block seed as additional information which in-

cludes the arrival time stamp and which is unique to the block data.

8. An information recording device according to Claim 1, wherein:

said secret-information decoding means is structured to execute decoding processing on data which is stored on said recording medium by using a binary sequence to disturb a string of bits constituting the secret information; and said secret-information decoding means executes decoding processing of the secret information by generating the binary sequence and executing arithmetic processing using the generated binary sequence and a playback signal from said recording medium.

9. An information recording device according to Claim 1, wherein said secret-information decoding means reads, from said recording medium, data which is recorded in a form converted in a predetermined manner from the secret information in units of a plurality of bits constituting the secret information, and executes decoding processing on the secret information by converting the read data again.

10. An information playback device for playing back information recorded on a recording medium, said information playback device comprising:

cryptosystem means for executing decryption processing on data read from said recording medium; and  
secret-information decoding means for reading secret information stored on said recording medium by executing a special data-reading process which is different from a process of reading content data stored on said recording medium;

wherein said cryptosystem means generates a content-decryption key by using, as a key-generating data, the secret information which is decoded after being read from said recording medium, and executes, based on the content-decryption key, the decryption processing on the read data.

11. An information playback device according to Claim 10, wherein:

the secret information includes a type of data among a stamper ID which is stored on said recording medium when said recording medium is produced and which is common to a plurality of recording media, a disk ID which is unique to each of the recording media, a content ID which is differently set for each content, and a cryptosystem key; and

said secret-information decoding means executes a decoding process on the read data.

12. An information playback device according to Claim 10, wherein said cryptosystem means uses the read secret information to generate the content-decryption key, and the read secret information is allowed to be used only in the generation of the content-decryption key which is executed in said cryptosystem means, without being stored in storage means which is readable from the outside of said information recording device.

13. An information playback device according to Claim 10, wherein:

said information recording device possesses node keys which are unique to nodes constituting a hierarchical tree structure having a plurality of different information recording devices as leaves;  
said cryptosystem means generates the content-encryption key based on the read secret information and decryption-key-generating data which is stored in said information recording device; and  
the decryption-key-generating data can be updated by using an enabling key block generated such that a node key is encrypted by using a key including at least one of a node key and a leaf key which are positioned at a lower level.

14. An information playback device according to Claim 13, wherein the decryption-key-generating data is one of a master key common to a plurality of information recording devices and a media key unique to a specified recording medium.

15. An information playback device according to Claim 13, wherein:

the decryption-key-generating data corresponds to a generation number as updating information; and  
when storing encrypted data on said recording medium, said cryptosystem means stores on said recording medium the generation number of the decryption-key-generating data as a recording-mode generation number.

16. An information playback device according to Claim 13, further comprising transport-stream processing means for adding an arrival time stamp to each of transport packets constituting a transport stream;

said cryptosystem means generates a block key as an encrypted key for block data composed of at least one transport packet to which

the arrival time stamp is added; and  
in decryption of the data to be stored on said recording medium, said cryptosystem means generates a block key as a decryption key based on data including the secret information, the decryption-key-generating data, and a block seed as additional information which includes the arrival time stamp and which is unique to the block data.

17. An information playback device according to Claim 10, wherein:

said secret-information decoding means is structured to execute decoding processing on data which is stored on said recording medium by using a binary sequence to disturb a string of bits constituting the secret information; and  
said secret-information decoding means executes decoding processing of the secret information by generating the binary sequence and executing arithmetic processing using the generated binary sequence and a playback signal from said recording medium.

18. An information playback device according to Claim 10, wherein said secret-information decoding means reads, from said recording medium, data which is recorded in a form converted in a predetermined manner from the secret information in units of a plurality of bits constituting the secret information, and executes decoding processing on the secret information by converting the read data again.

19. An information recording method for recording information on a recording medium, said information recording method comprising:

a secret-information decoding step which reads secret information stored on said recording medium by executing a special data-reading process which is different from a process of reading content data stored on said recording medium; and  
a cryptosystem step which generates a content-encryption key by using, as a key-generating data, the secret information which is decoded after being read from said recording medium in said secret-information decoding step, and executes, based on the content-encryption key, the encryption processing on the data to be stored.

20. An information recording method according to Claim 19, wherein:

the secret information includes a type of data among a stamper ID which is stored on said re-

recording medium when said recording medium is produced and which is common to a plurality of recording media, a disk ID which is unique to each of the recording media, a content ID which is differently set for each content, and a cryptosystem key; and  
 said secret-information decoding means executes a decoding process on the read data.

21. An information recording method according to Claim 19, wherein said cryptosystem step includes a step which uses the read secret information to generate the content-encryption key, and the read secret information is allowed to be used only in the generation of the content-encryption key which is executed in said cryptosystem step, without being stored in storage means which is readable from the outside of said information recording device.

22. An information recording method according to Claim 19, wherein:

said cryptosystem step includes a step which generates the content-encryption key based on the read secret information and encryption-key-generating data which is stored in said information recording device; and  
 the encryption-key-generating data can be updated by an enabling key block generated such that in a hierarchical tree structure having a plurality of different information recording devices as leaves, branches as nodes, and unique keys set for said leaves and said nodes, a node key is encrypted by using a key including at least one of a node key and a leaf key which are positioned at a lower level.

23. An information recording method according to Claim 22, wherein the encryption-key-generating data is one of a master key common to a plurality of information recording devices and a media key unique to a specified recording medium.

24. An information recording method according to Claim 22, wherein:

the encryption-key-generating data corresponds to a generation number as updating information; and  
 when storing encrypted data on said recording medium, said cryptosystem step stores on said recording medium the generation number of the encryption-key-generating data as a recording-mode generation number.

25. An information recording method according to Claim 22, further comprising a transport-stream processing step for adding an arrival time stamp to

each of transport packets constituting a transport stream;

said cryptosystem step includes a step which generates a block key as an encrypted key for block data composed of at least one transport packet to which the arrival time stamp is added; and  
 in encryption of the data to be stored on said recording medium, said cryptosystem step generates a block key as an encryption key based on data including the secret information, the encryption-key-generating data, and a block seed as additional information which includes the arrival time stamp and which is unique to the block data.

26. An information recording method according to Claim 19, wherein:

said secret-information decoding step includes a step which executes decoding processing on data which is stored on said recording medium by using a binary sequence to disturb a string of bits constituting the secret information; and  
 said secret-information decoding step executes decoding processing of the secret information by generating the binary sequence and executing arithmetic processing using the generated binary sequence and a playback signal from said recording medium.

27. An information recording method according to Claim 19, wherein said secret-information decoding step reads, from said recording medium, data which is recorded in a form converted in a predetermined manner from the secret information in units of a plurality of bits constituting the secret information, and executes decoding processing on the secret information by converting the read data again.

28. An information playback method for playing back information from a recording medium, said information playback method comprising:

a secret-information decoding step which reads secret information stored on said recording medium by executing a special data-reading process which is different from a process of reading content data stored on said recording medium; and  
 a decryption step which generates a content-decryption key by using, as a key-generating data, the secret information which is decoded after being read from said recording medium in said secret-information decoding step, and executes, based on the content-decryption key, the decryption processing on the read data.

29. An information playback method according to Claim 28, wherein:

the secret information includes a type of data among a stamper ID which is stored on said recording medium when said recording medium is produced and which is common to a plurality of recording media, a disk ID which is unique to each of the recording media, a content ID which is differently set for each content, and a cryptosystem key; and  
said secret-information decoding step executes a decoding process on the read data.

30. An information playback method according to Claim 28, wherein said decryption step includes a step which uses the read secret information to generate the content-decryption key, and the read secret information is allowed to be used only in the generation of the content-decryption key which is executed in said cryptosystem means, without being stored in storage means which is readable from the outside of said information recording device.

31. An information playback method according to Claim 28, wherein:

said decryption step includes a step which generates the content-decryption key based on the read secret information and decryption-key-generating data which is stored in said information recording device; and  
the decryption-key-generating data can be updated by an enabling key block generated such that in a hierarchical tree structure having a plurality of different information recording devices as leaves, branches as nodes, and unique keys set for said leaves and said nodes, a node key is encrypted by using a key including at least one of a node key and a leaf key which are positioned at a lower level.

32. An information playback method according to Claim 31, wherein the decryption-key-generating data is one of a master key common to a plurality of information playback devices and a media key unique to a specified recording medium.

33. An information playback method according to Claim 31, wherein:

the decryption-key-generating data corresponds to a generation number as updating information; and  
when storing encrypted data on said recording medium, said decryption step stores on said recording medium the generation number of the decryption-key-generating data as a recording-

mode generation number.

34. An information playback method according to Claim 31, further comprising a transport-stream processing step for adding an arrival time stamp to each of transport packets constituting a transport stream;

said decryption step includes a step which generates a block key as an encryption key for block data composed of at least one transport packet to which the arrival time stamp is added; and  
in playback of the data to be stored on said recording medium, said decryption step generates a block key as a decryption key based on data including the secret information, the decryption-key-generating data, and a block seed as additional information which includes the arrival time stamp and which is unique to the block data.

35. An information playback method according to Claim 28, wherein:

said secret-information decoding step includes a step which executes decoding processing on data which is stored on said recording medium by using a binary sequence to disturb a string of bits constituting the secret information; and  
said secret-information decoding step executes decoding processing of the secret information by generating the binary sequence and executing arithmetic processing using the generated binary sequence and a playback signal from said recording medium.

36. An information playback method according to Claim 28, wherein said secret-information decoding step reads, from said recording medium, data which is recorded in a form converted in a predetermined manner from the secret information in units of a plurality of bits constituting the secret information, and executes decoding processing on the secret information by converting the read data again.

37. An information recording medium containing:

secret information which can be played back only by executing a special data-reading process different from an ordinary data-reading process; and  
an encrypted content which can be decrypted by using a cryptosystem key which can be generated by using said secret information.

38. An information recording medium according to Claim 37, wherein said secret information includes a type of data among a stamper ID common to a

plurality of recording media, a disk ID which is unique to each of the recording media, a content ID which is differently set for each content, and a cryptosystem key.

5

39. A program providing medium for providing a computer program which controls a computer system to execute information-recording processing for recording information on a recording medium, said computer program comprising:

10

a secret-information decoding step which reads secret information stored on said recording medium by executing a special data-reading process which is different from a process of reading content data stored on said recording medium; and

15

a cryptosystem step which generates a content-encryption key by using, as a key-generating data, the secret information which is decoded after being read from said recording medium in said secret-information decoding step, and executes, based on the content-encryption key, the encryption processing on the data to be stored.

20

25

40. A program providing medium for providing a computer program which controls a computer system to execute information-playback processing for playing back information stored on a recording medium, said computer program comprising:

30

a secret-information decoding step which reads secret information stored on said recording medium by executing a special data-reading process which is different from a process of reading content data stored on said recording medium; and

35

a decryption step which generates a content-decryption key by using, as a key-generating data, the secret information which is decoded after being read from said recording medium in said secret-information decoding step, and executes, based on the content-decryption key, the decryption processing on the read data.

40

45

50

55

FIG. 1

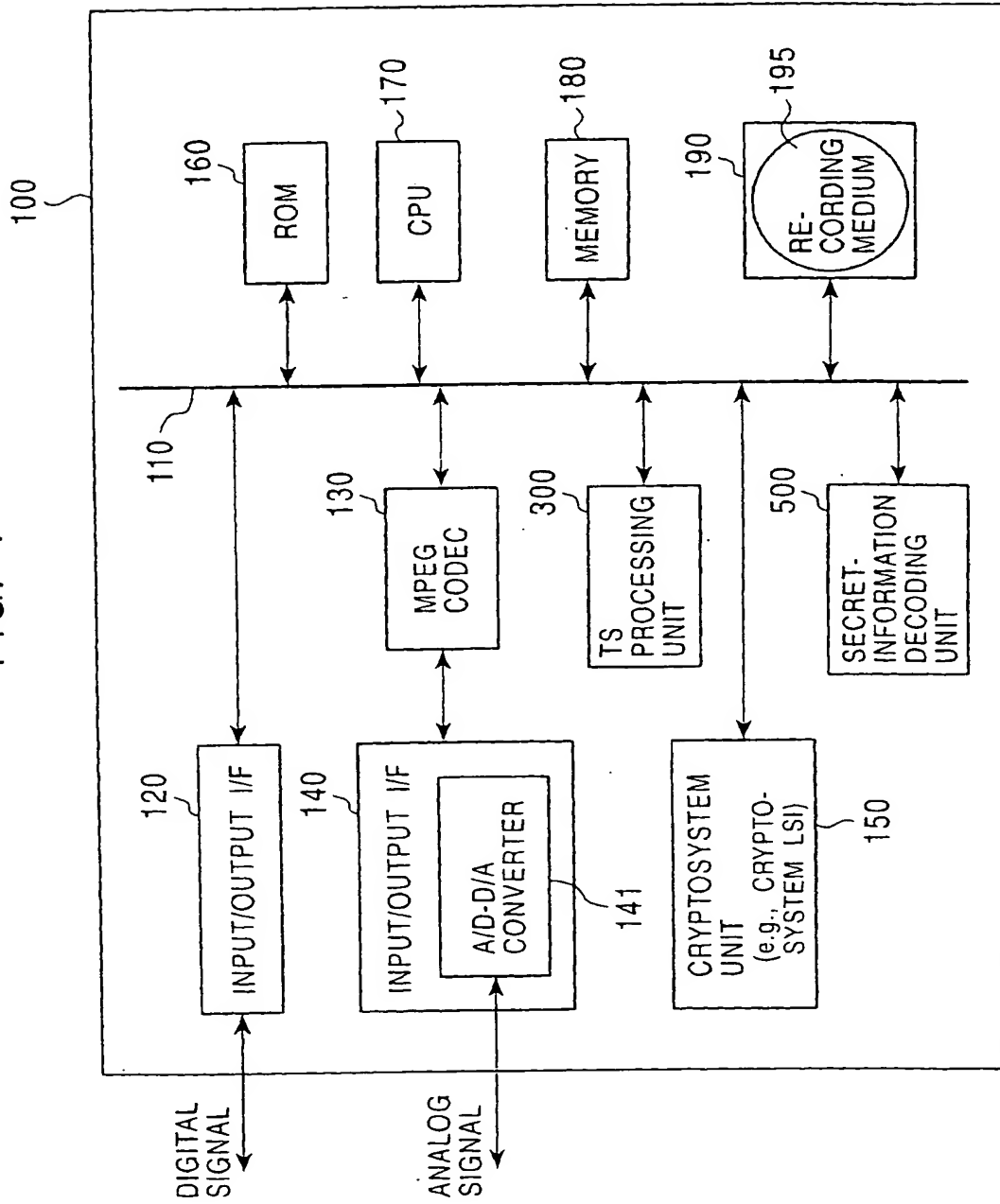


FIG. 2

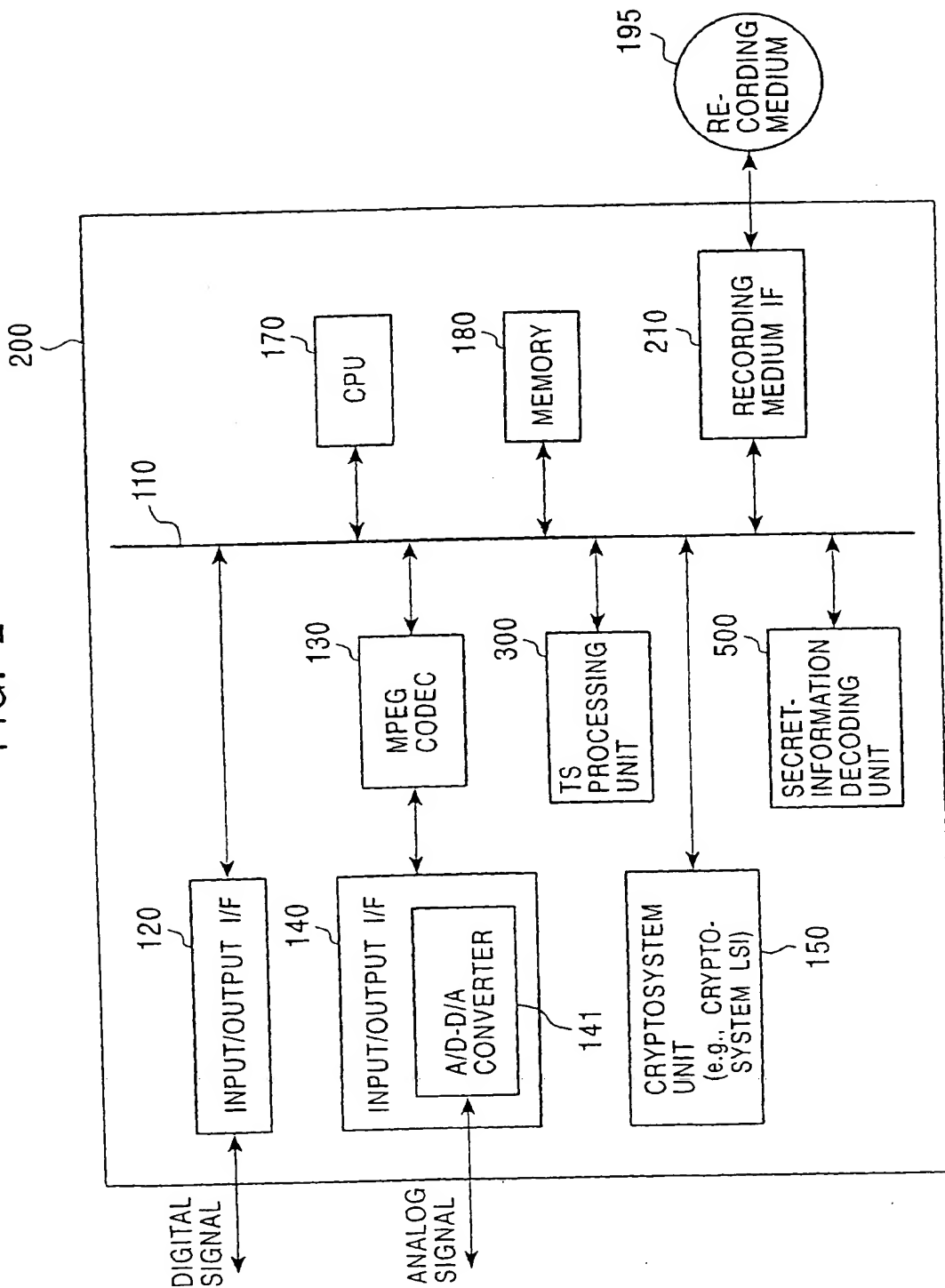


FIG. 3A

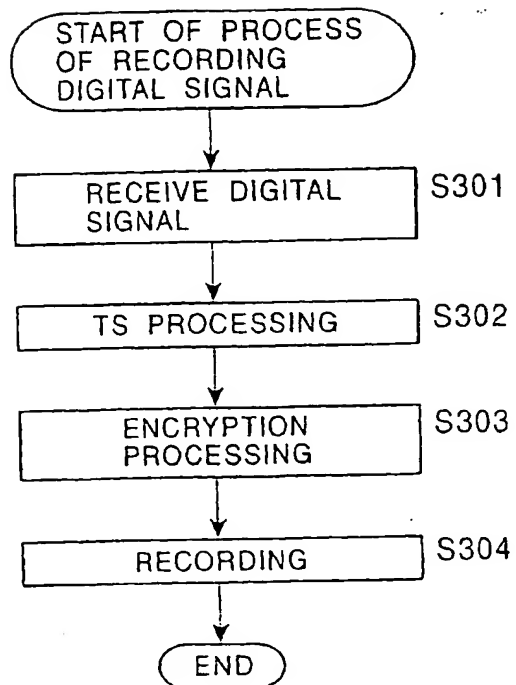


FIG. 3B

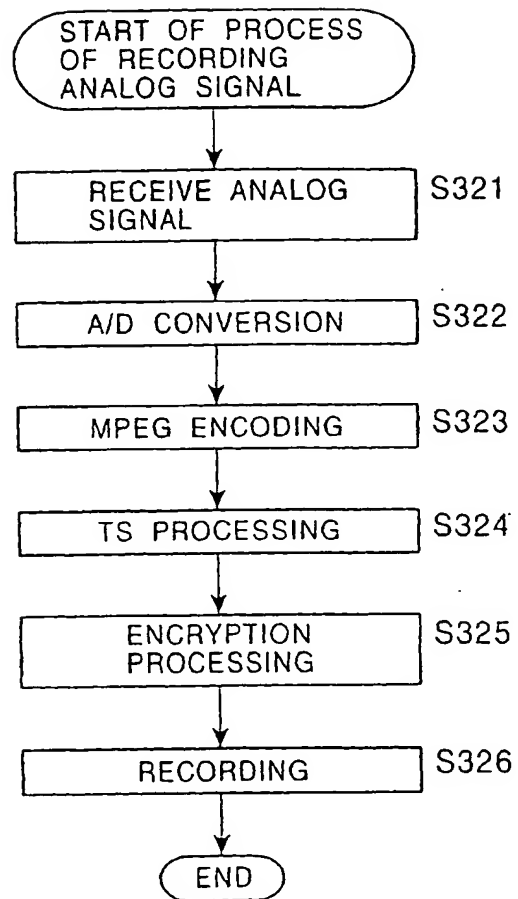


FIG. 4A

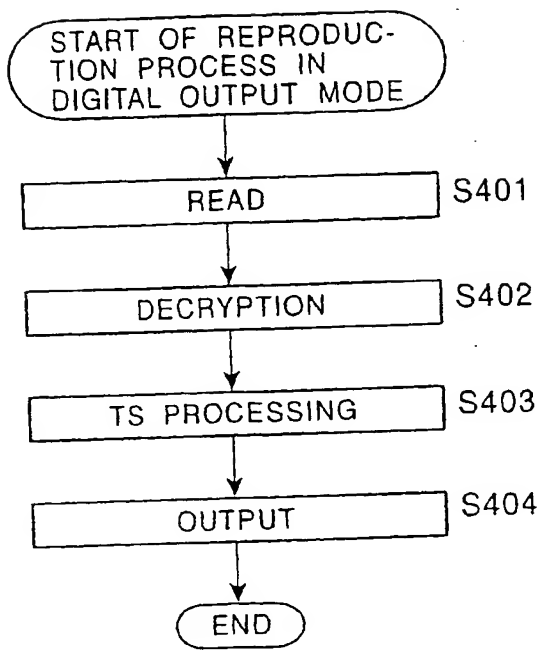


FIG. 4B

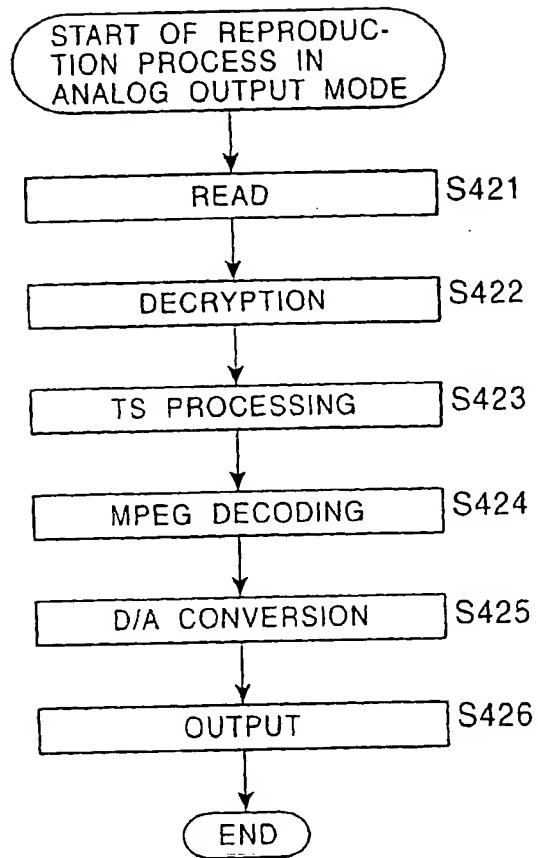


FIG. 5

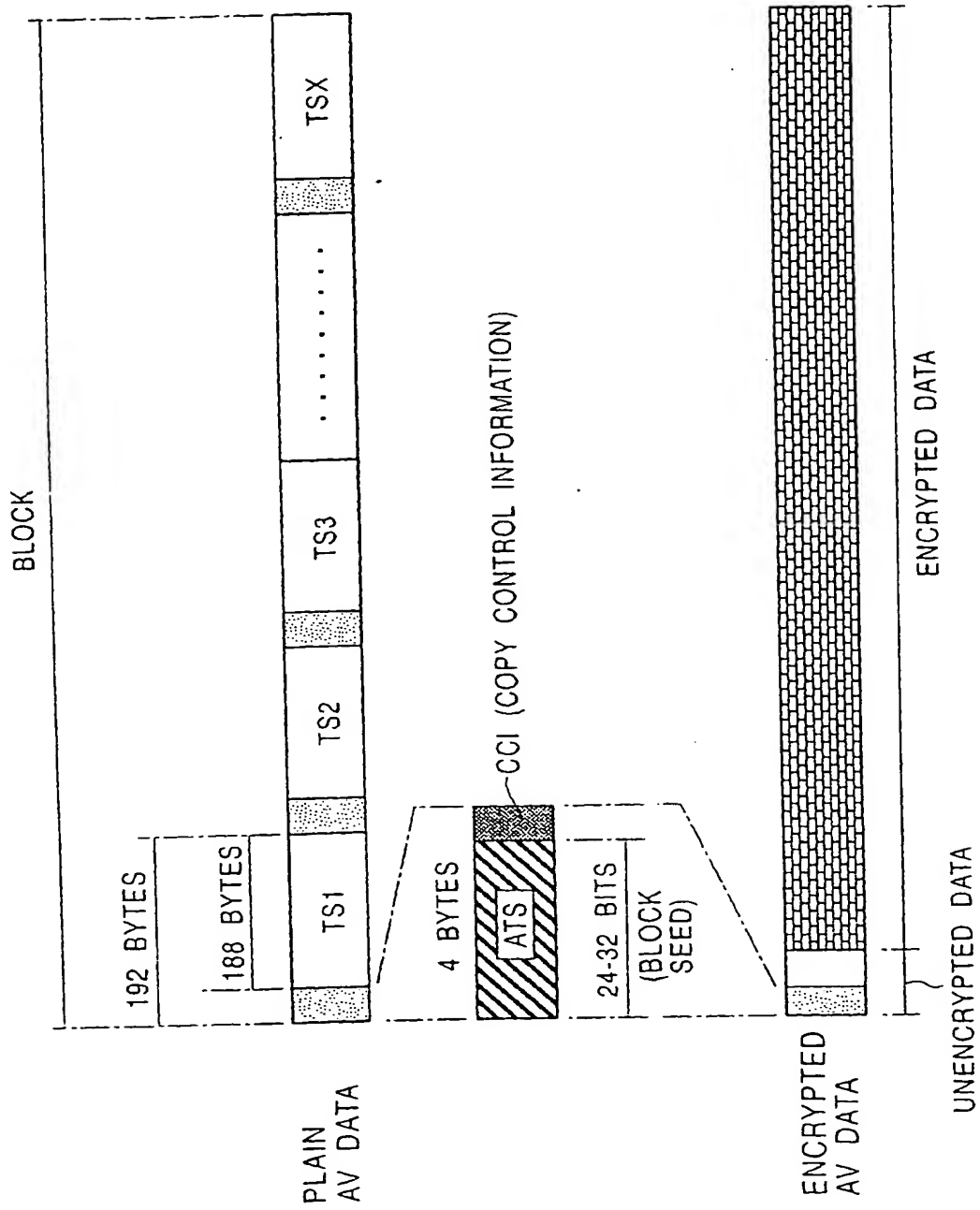
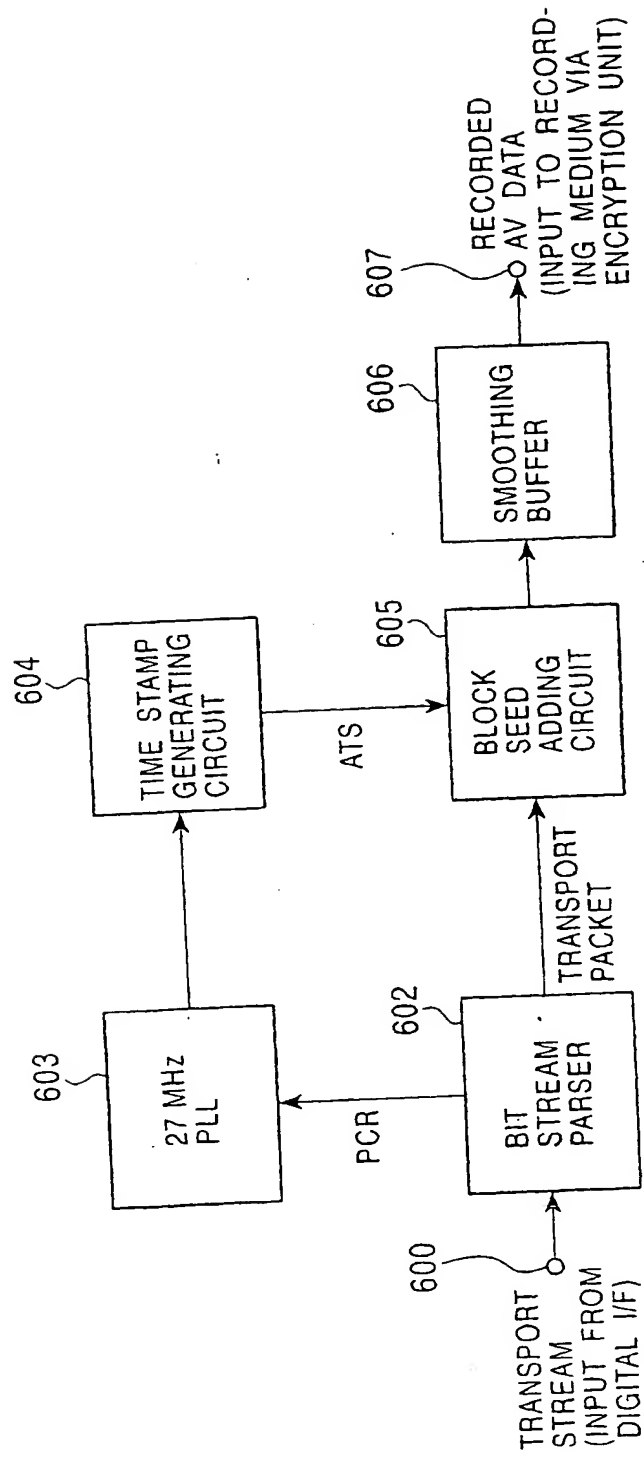


FIG. 6



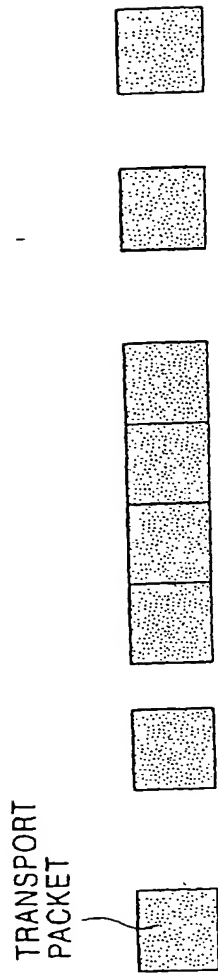


FIG. 7A

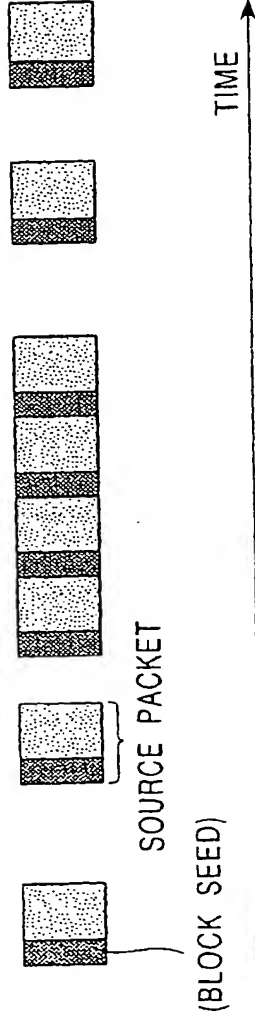


FIG. 7B

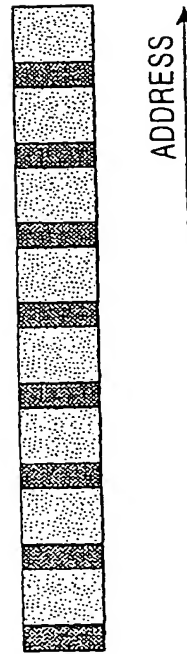


FIG. 7C

FIG. 8

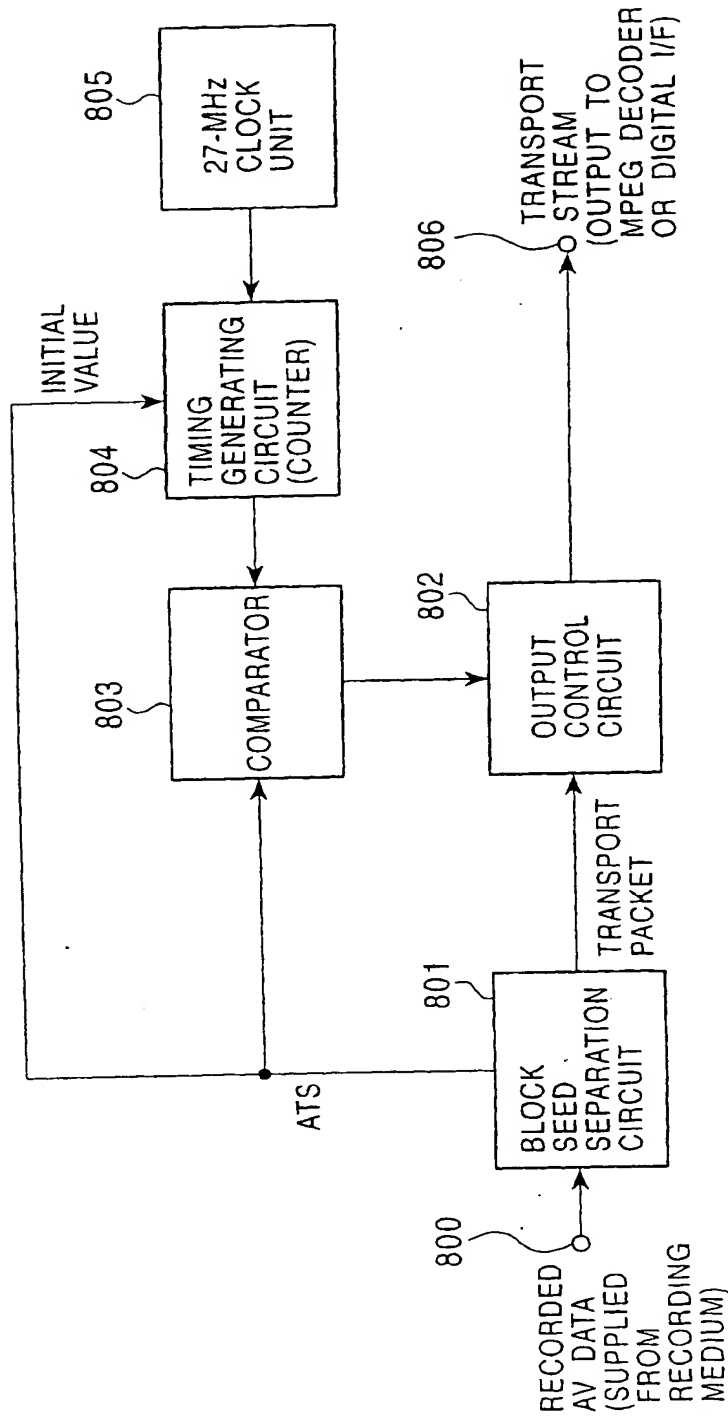


FIG. 9

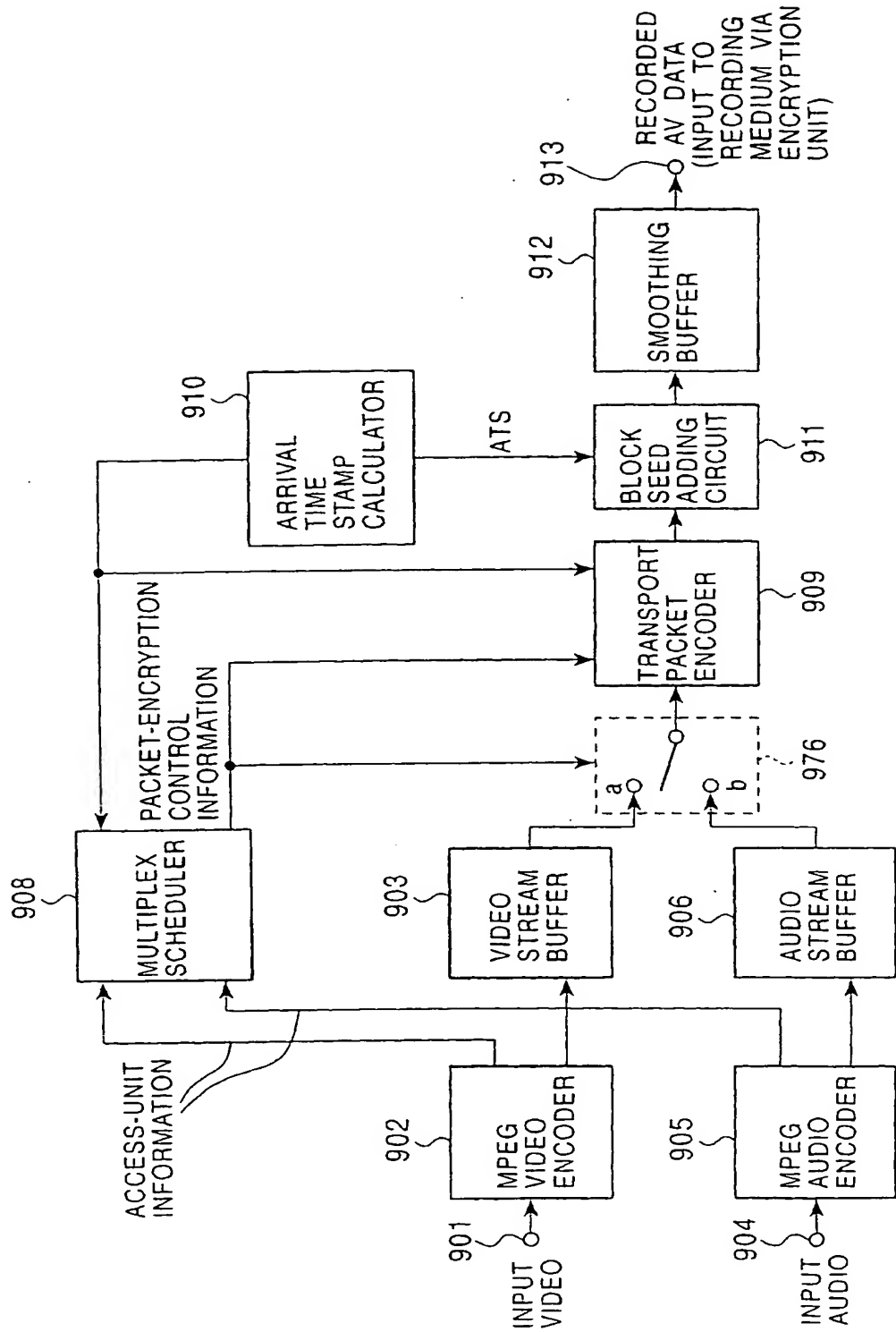


FIG. 10

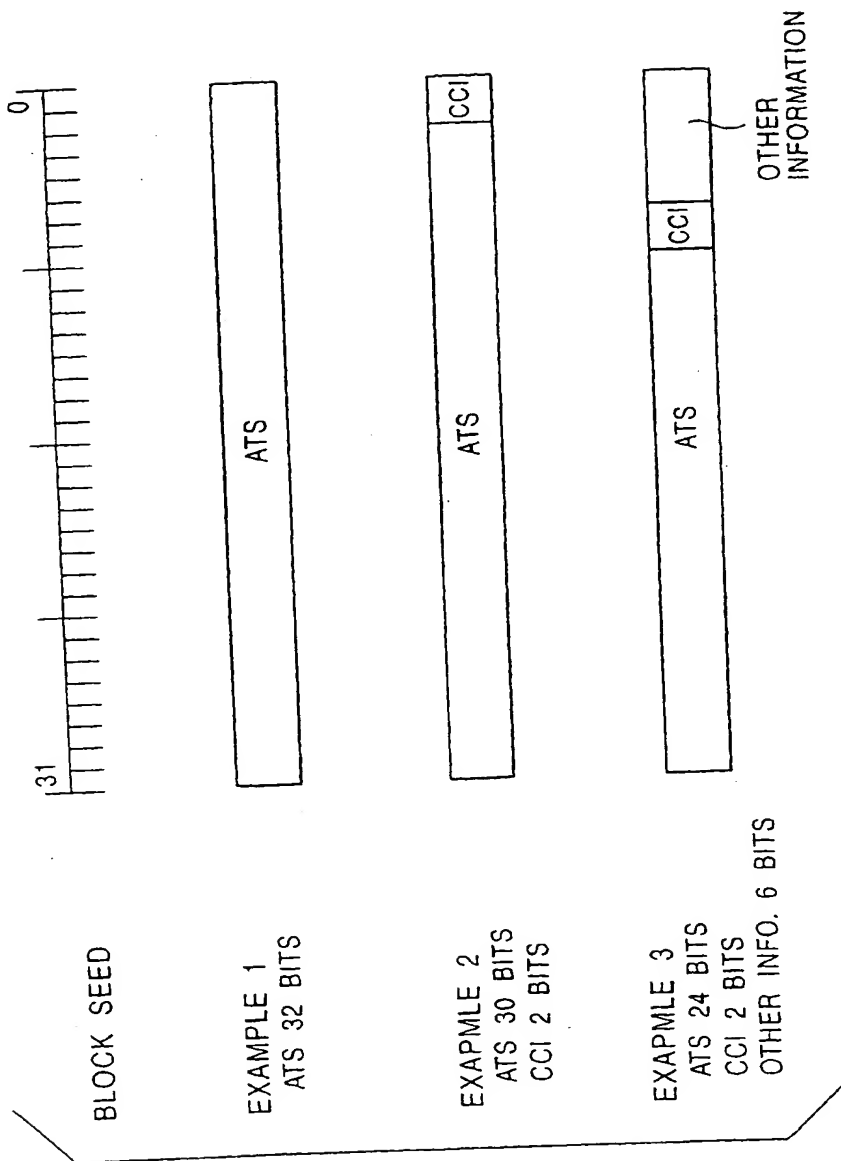


FIG. 11

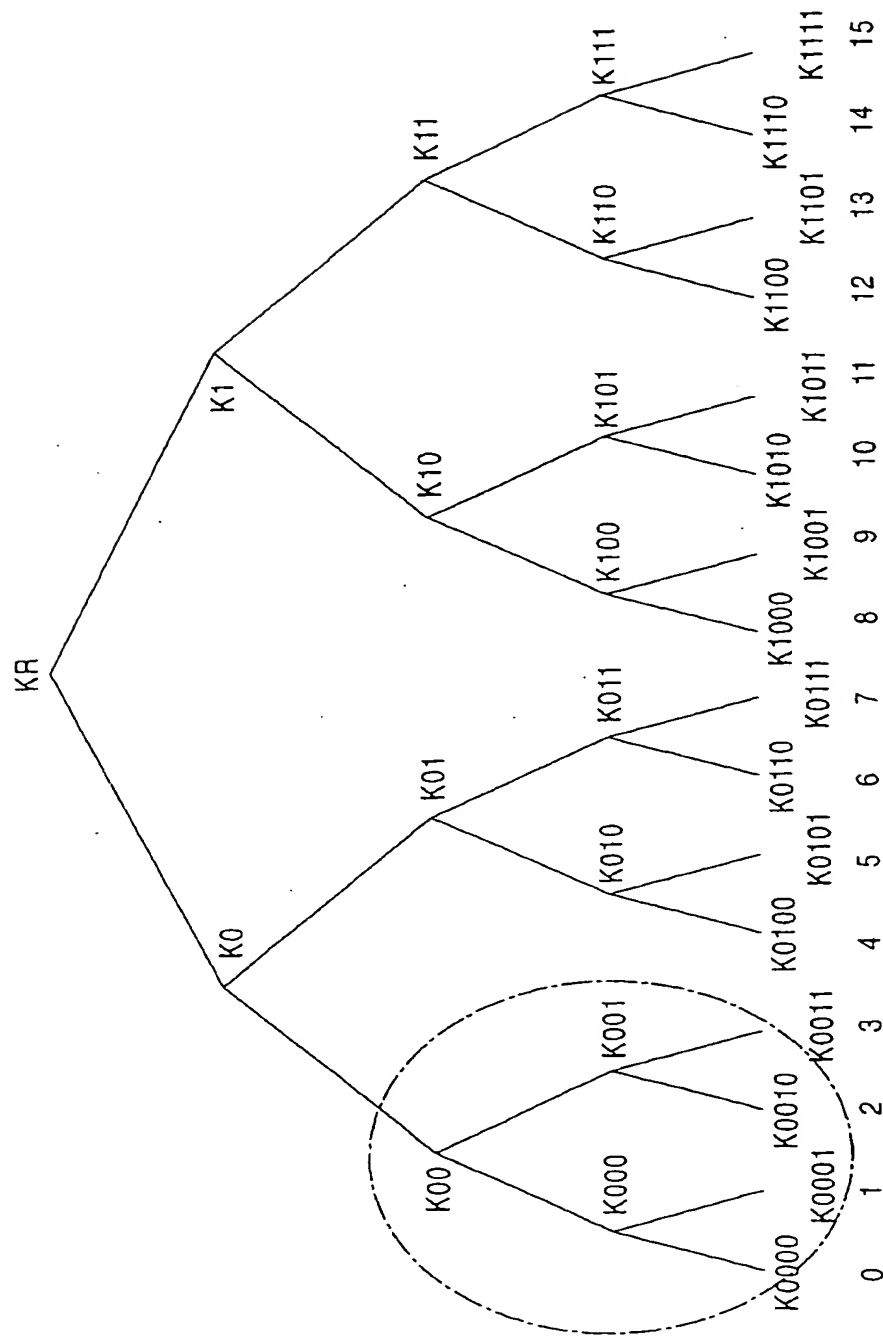


FIG. 12A

GENERATION : t	
INDEX	ENCRYPTION KEY
0	$\text{Enc}(K(t)0, K(t)R)$
00	$\text{Enc}(K(t)00, K(t)0)$
000	$\text{Enc}(K000, K(t)00)$
001	$\text{Enc}(K(t)001, K(t)00)$
0010	$\text{Enc}(K0010, K(t)001)$

FIG. 12B

GENERATION : t	
INDEX	ENCRYPTION KEY
000	$\text{Enc}(K000, K(t)00)$
001	$\text{Enc}(K(t)001, K(t)00)$
0010	$\text{Enc}(K0010, K(t)001)$

FIG. 13

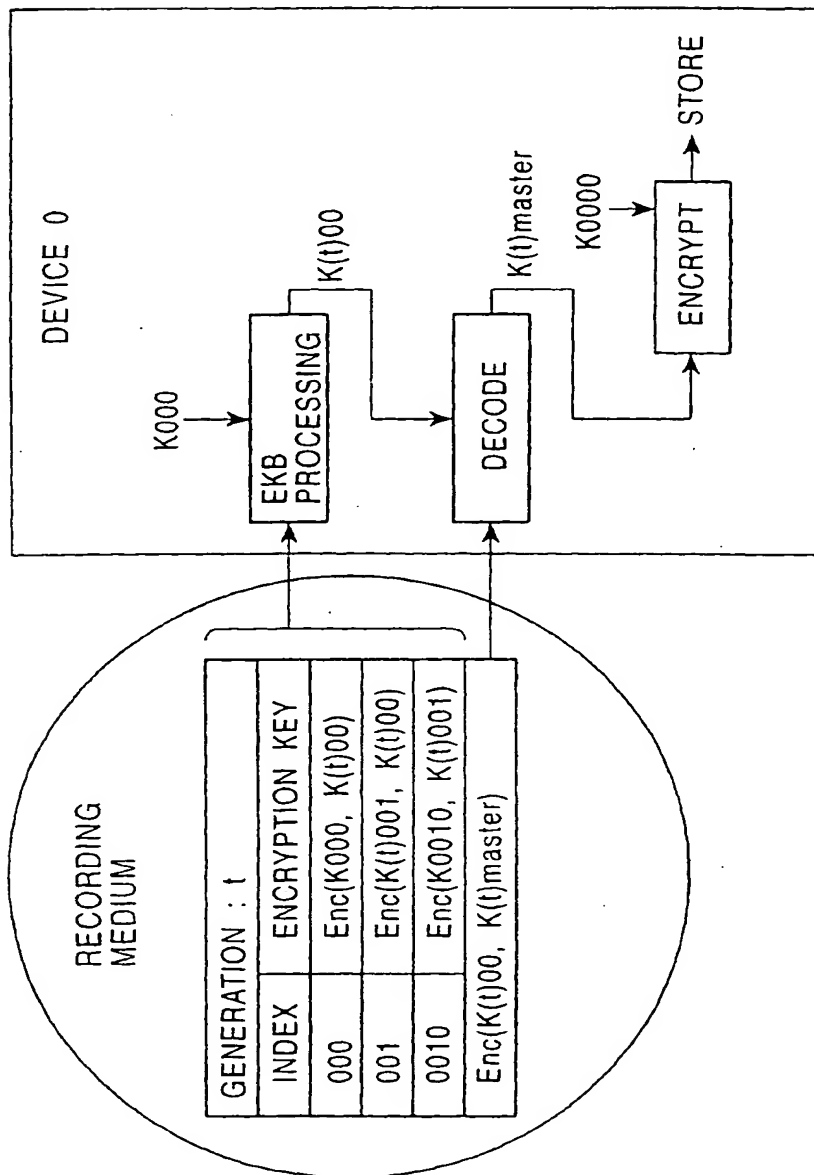


FIG. 14

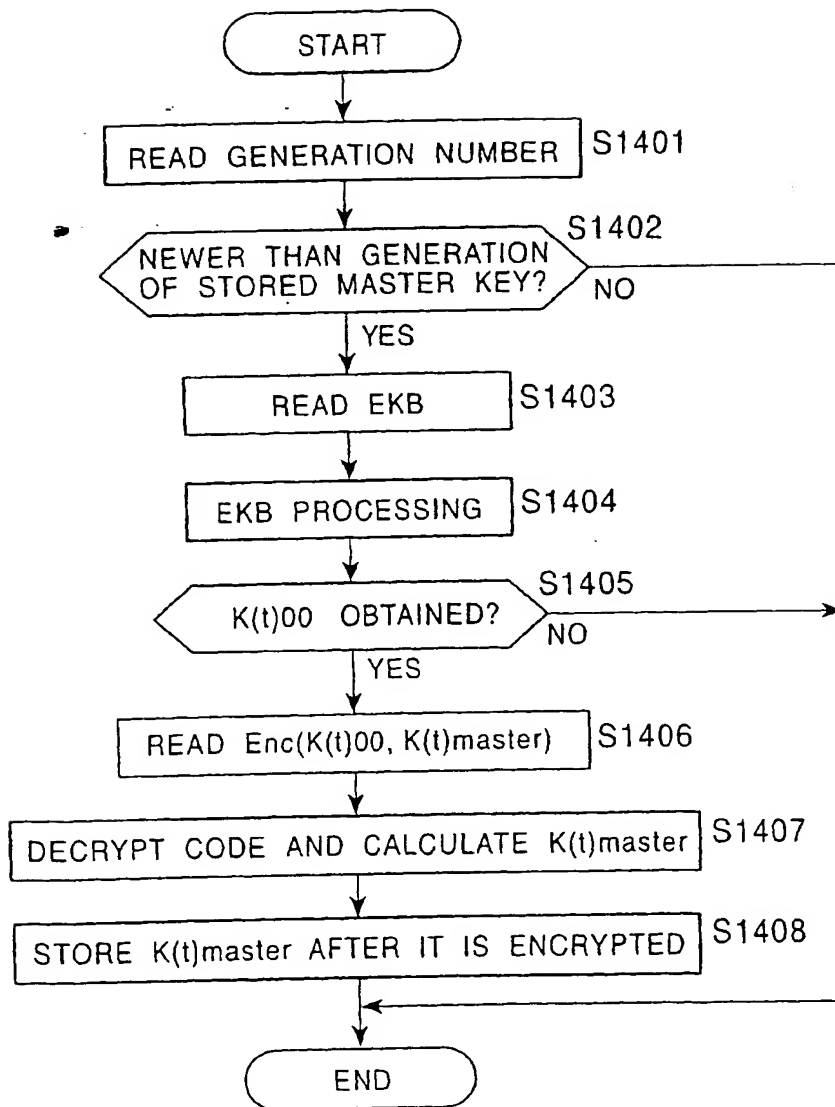


FIG. 15

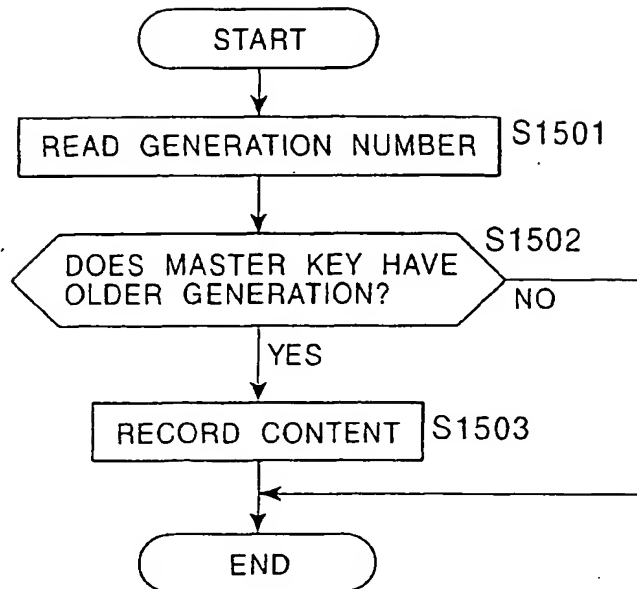


FIG. 16

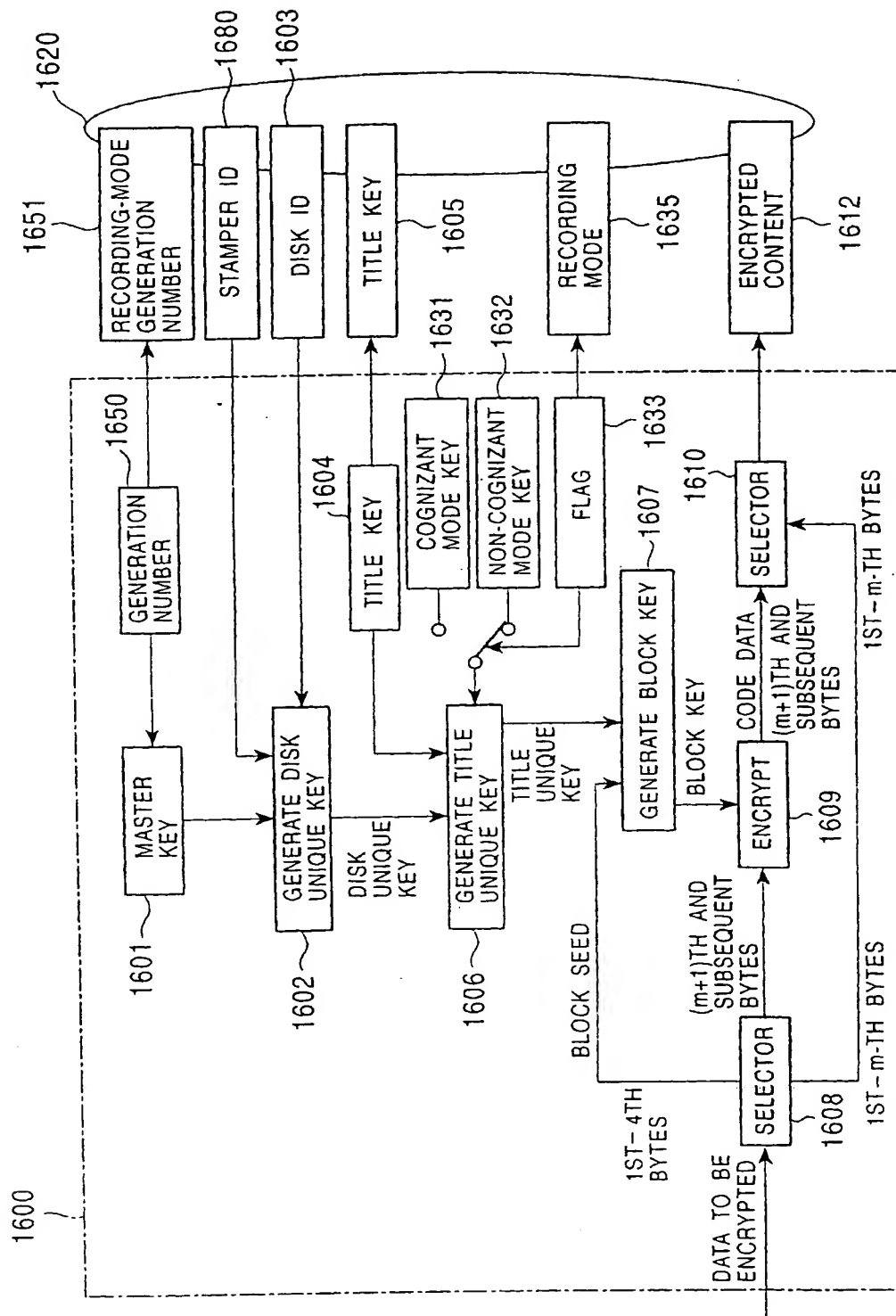


FIG. 17

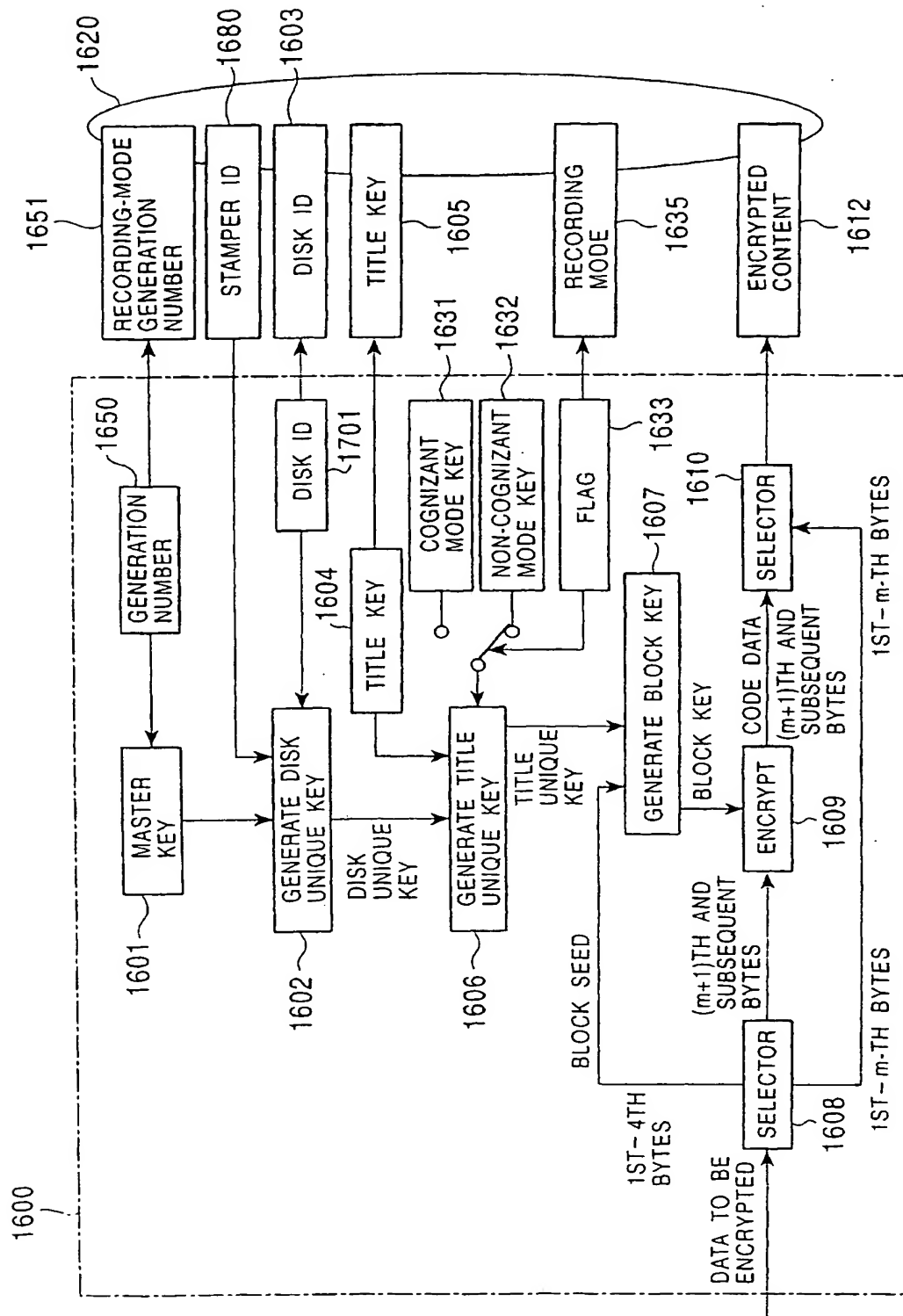


FIG. 18

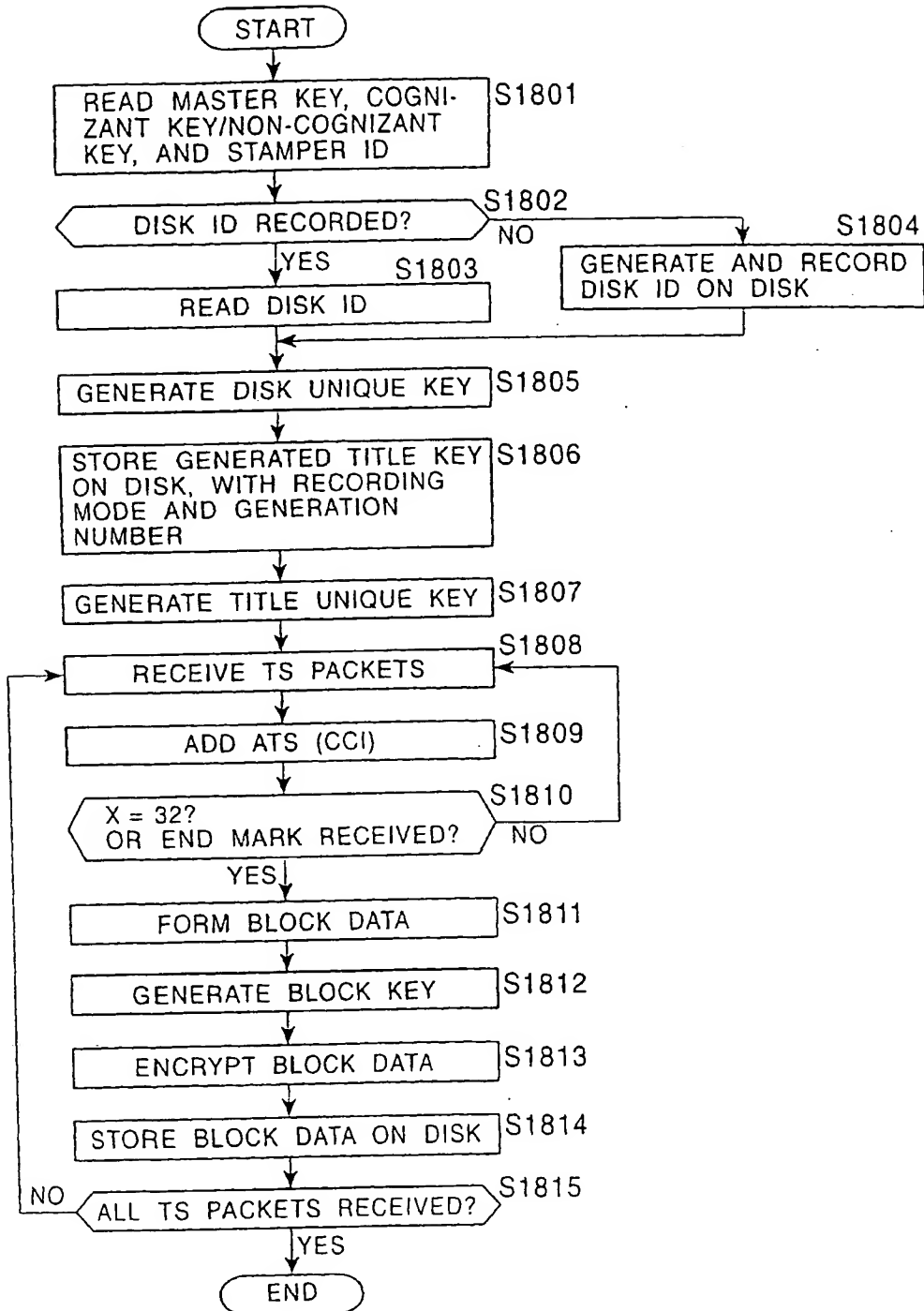


FIG. 19A

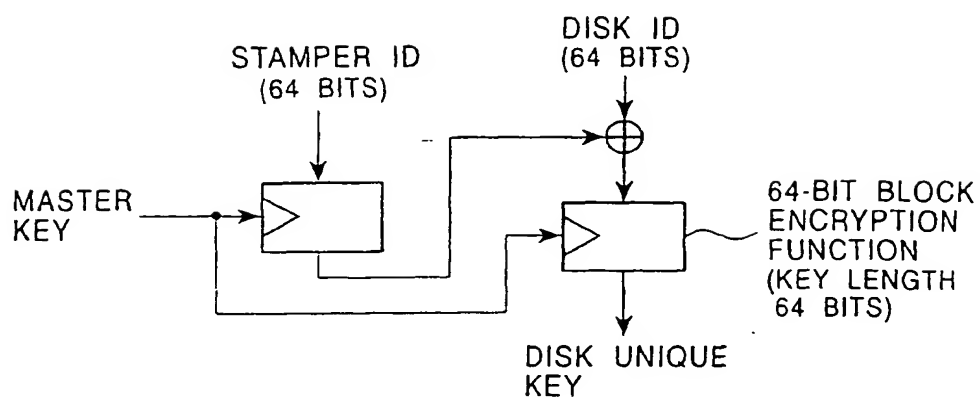


FIG. 19B

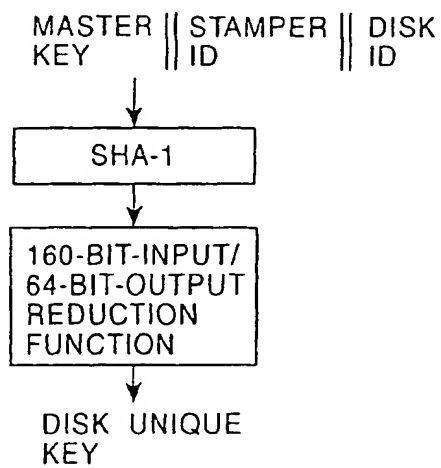


FIG. 20

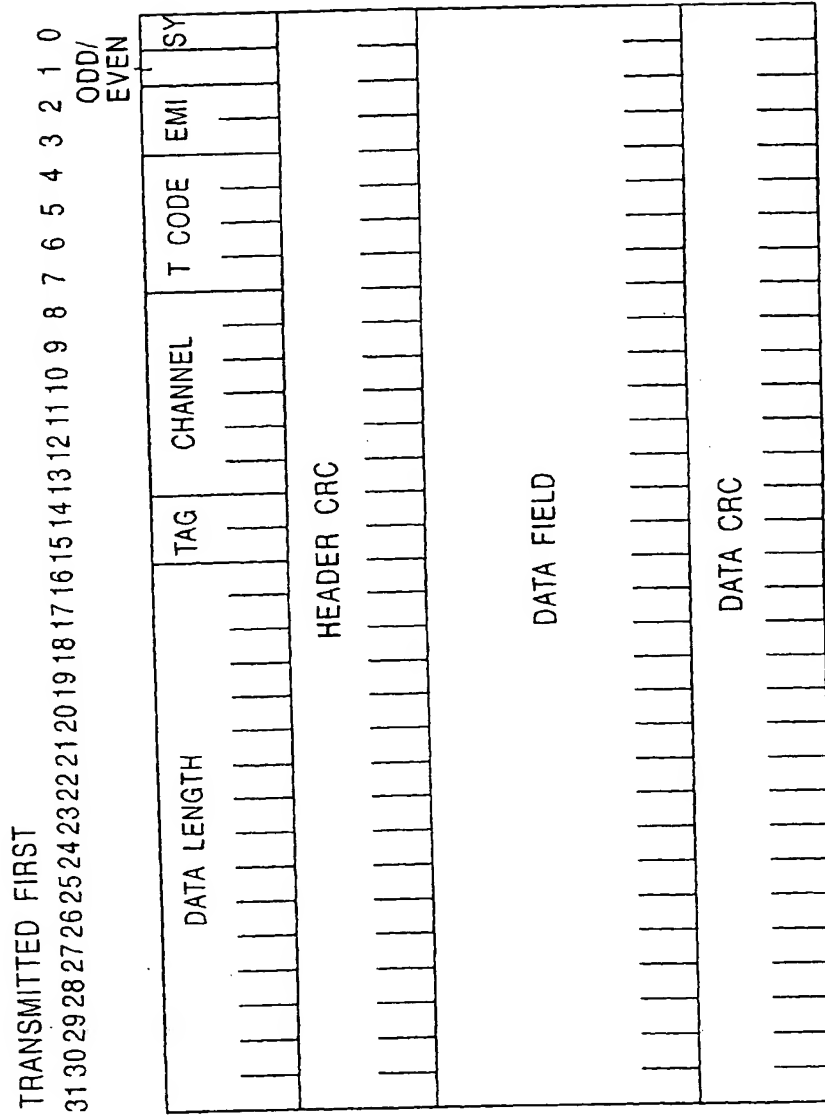


FIG. 21

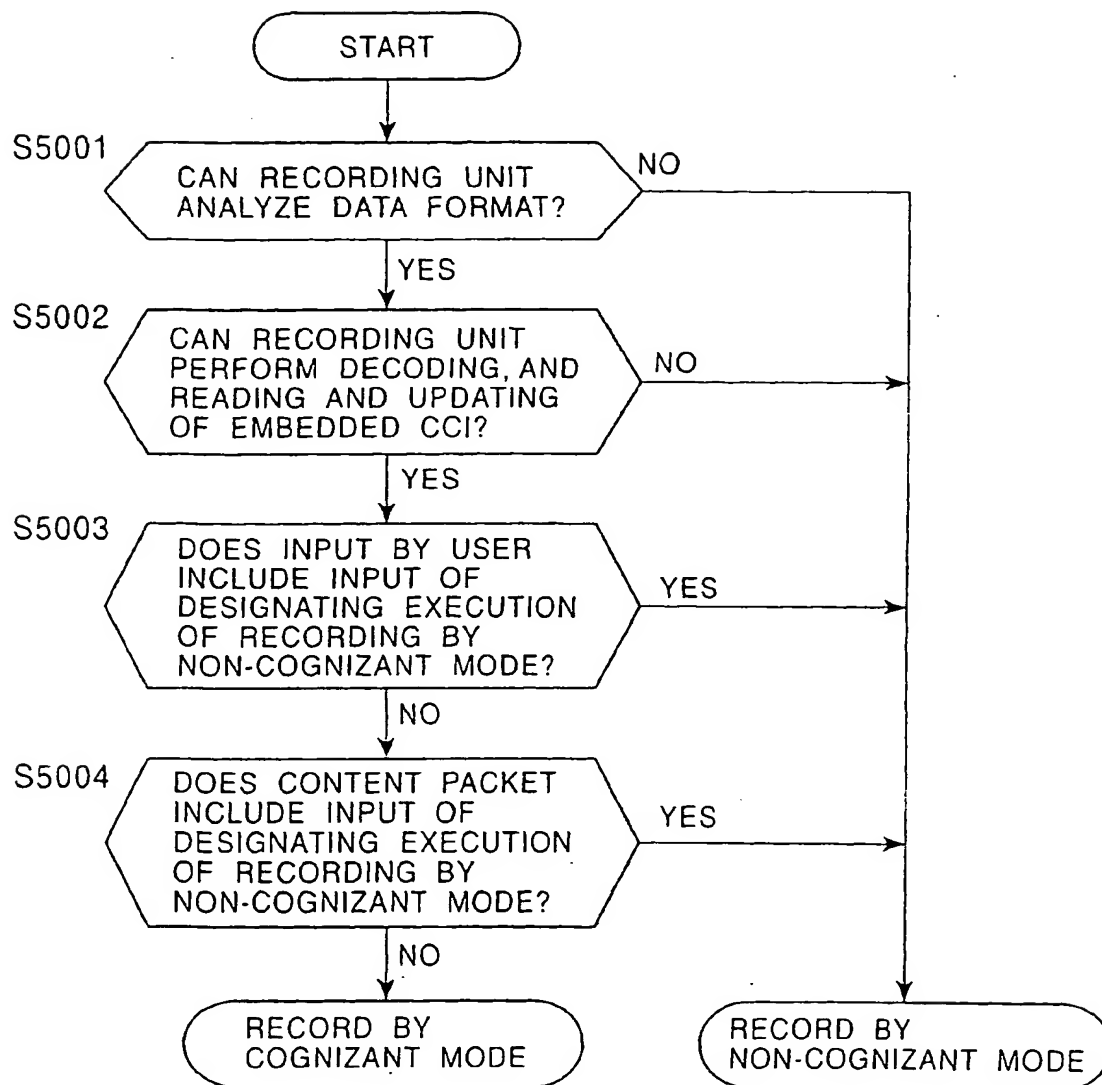


FIG. 22A

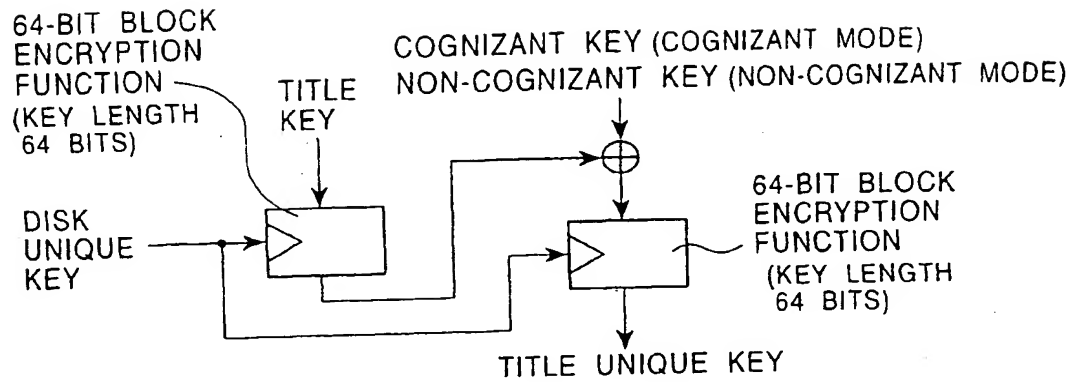


FIG. 22B

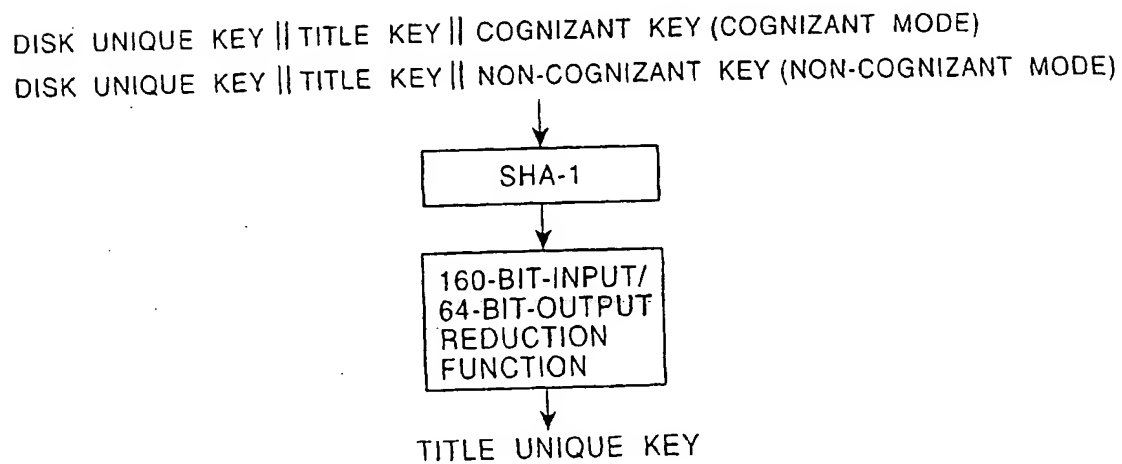


FIG. 23A

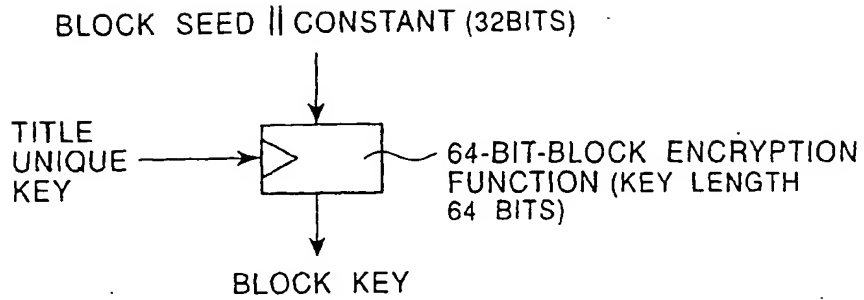


FIG. 23B

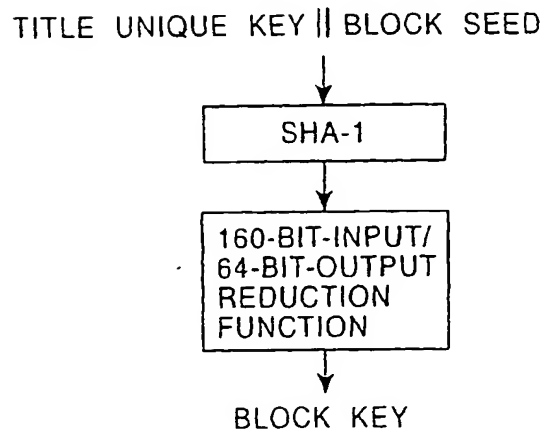


FIG. 24

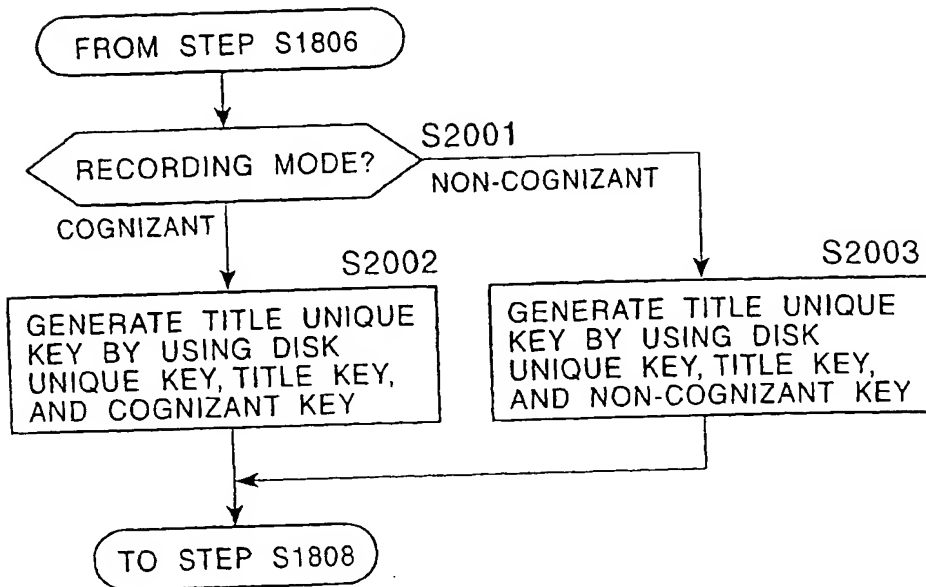


FIG. 25

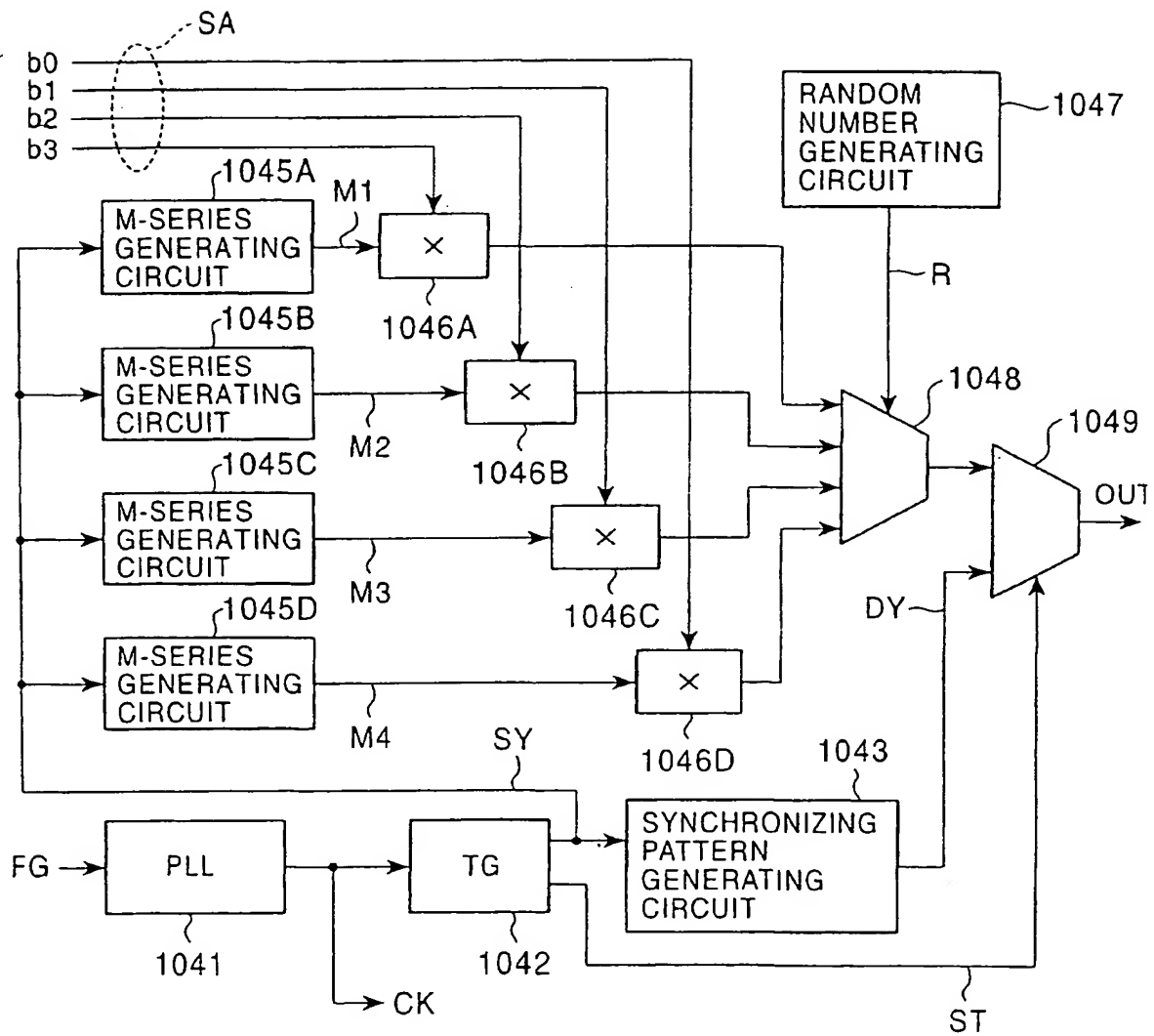


FIG. 26

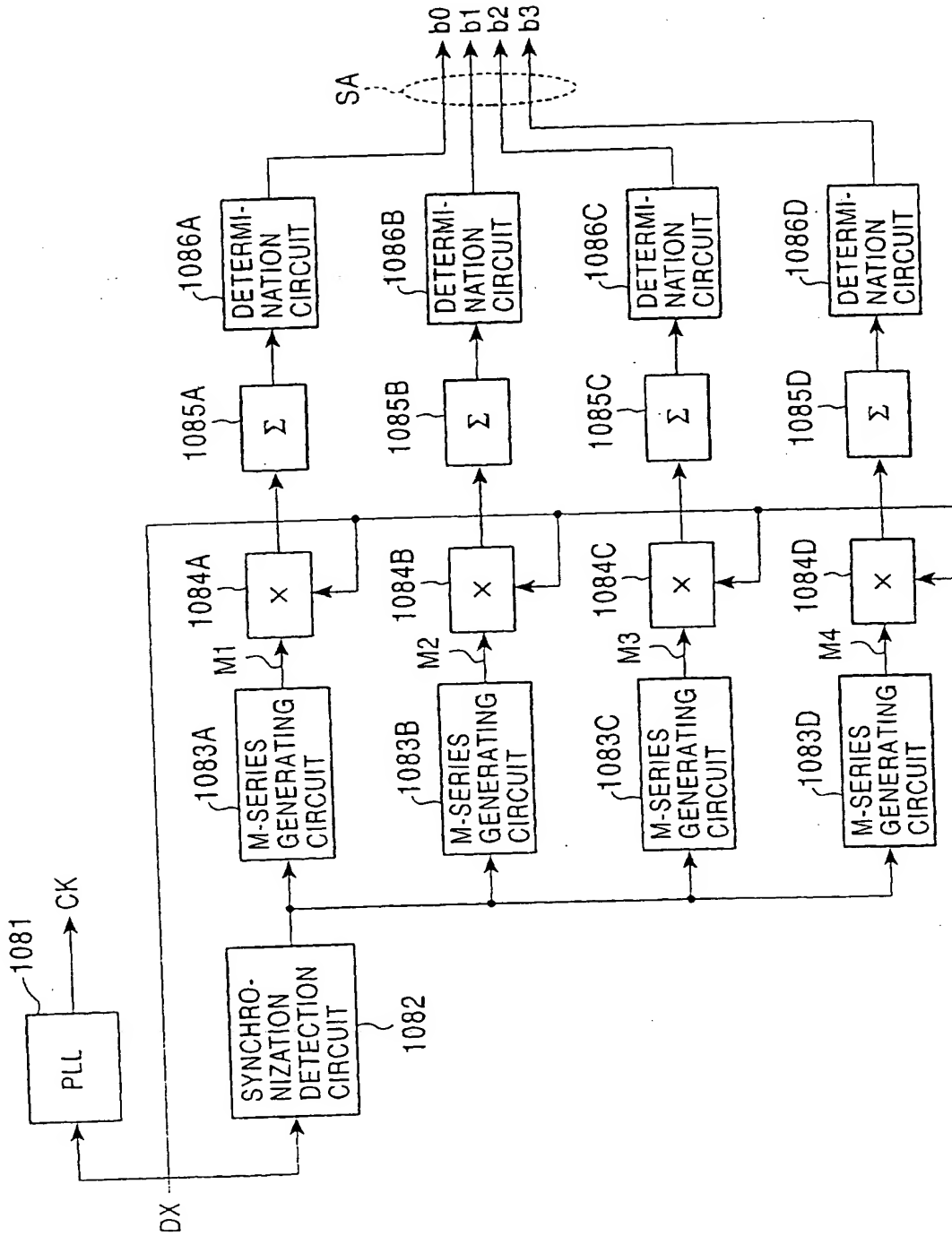


FIG. 27

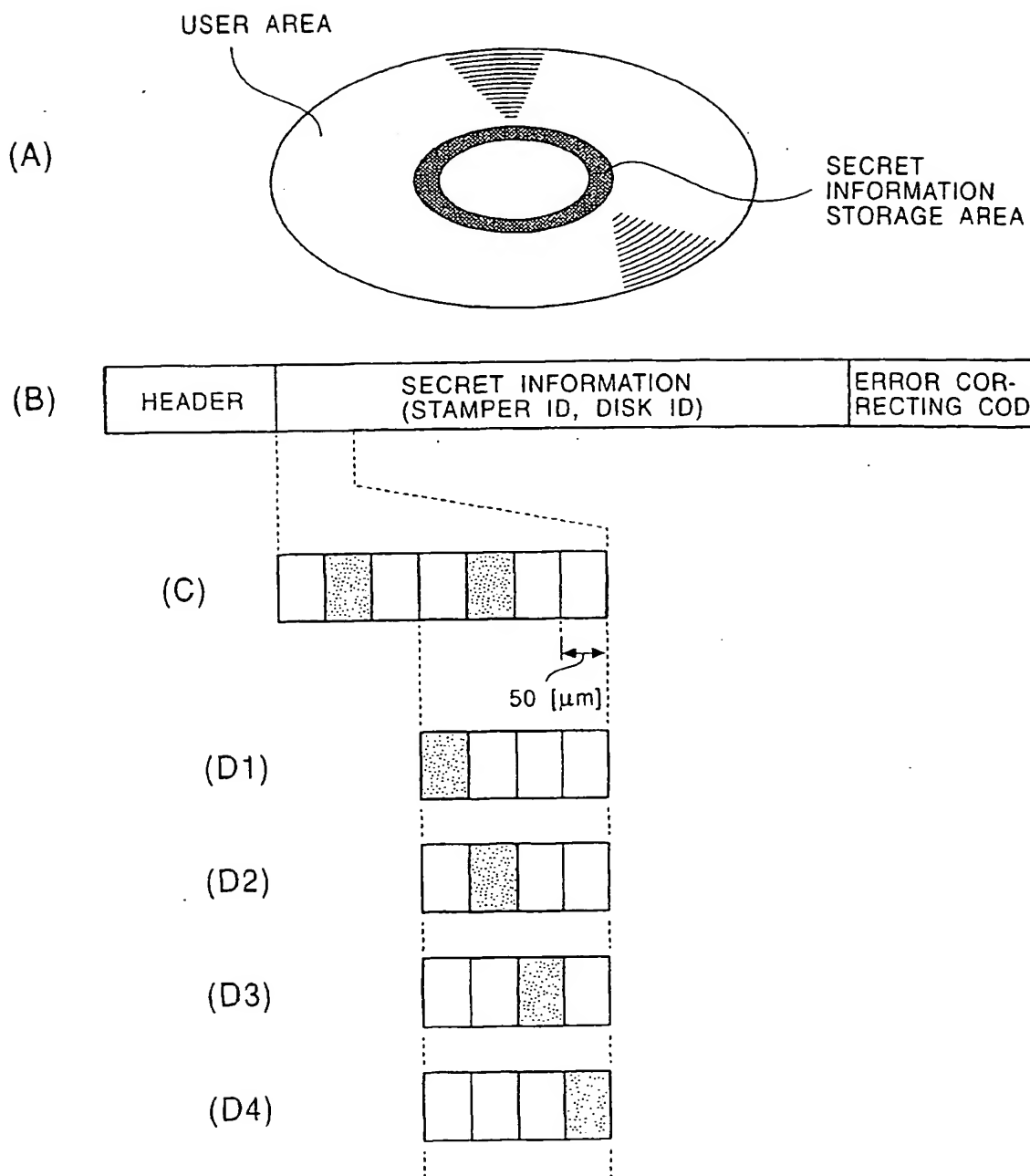


FIG. 28

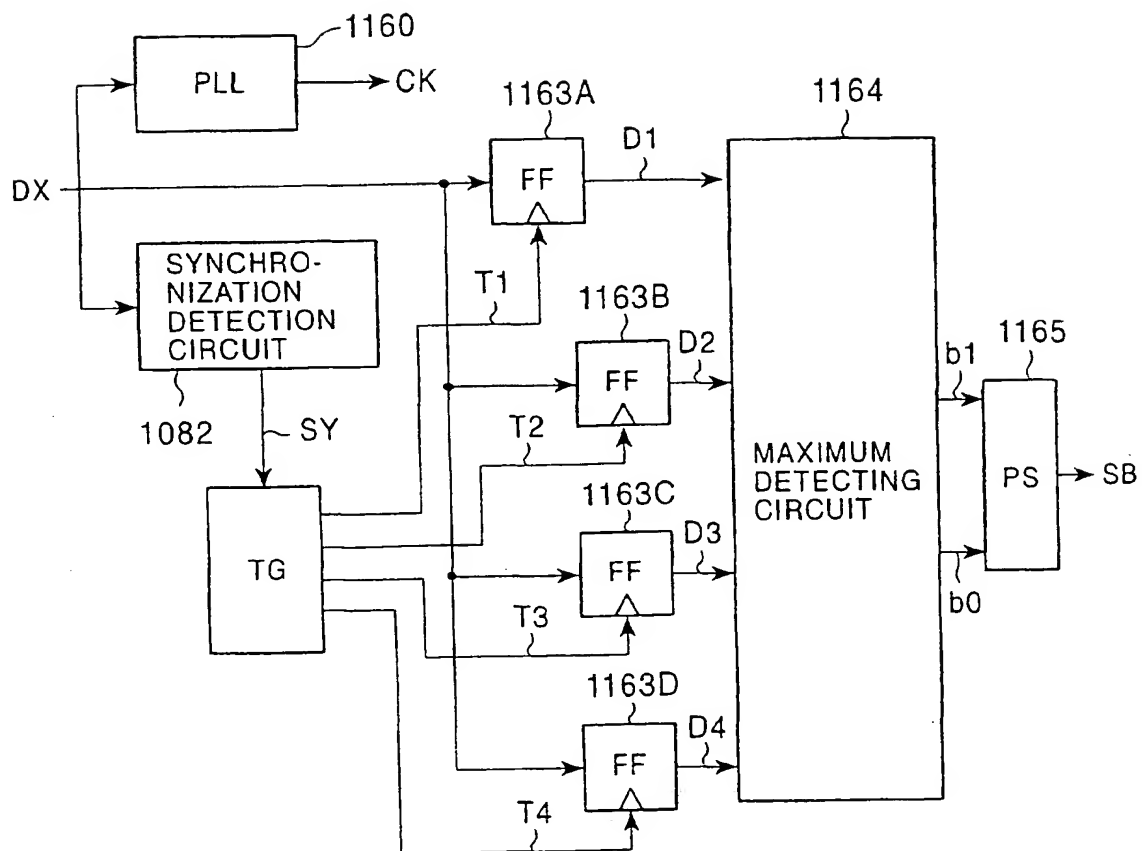


FIG. 29

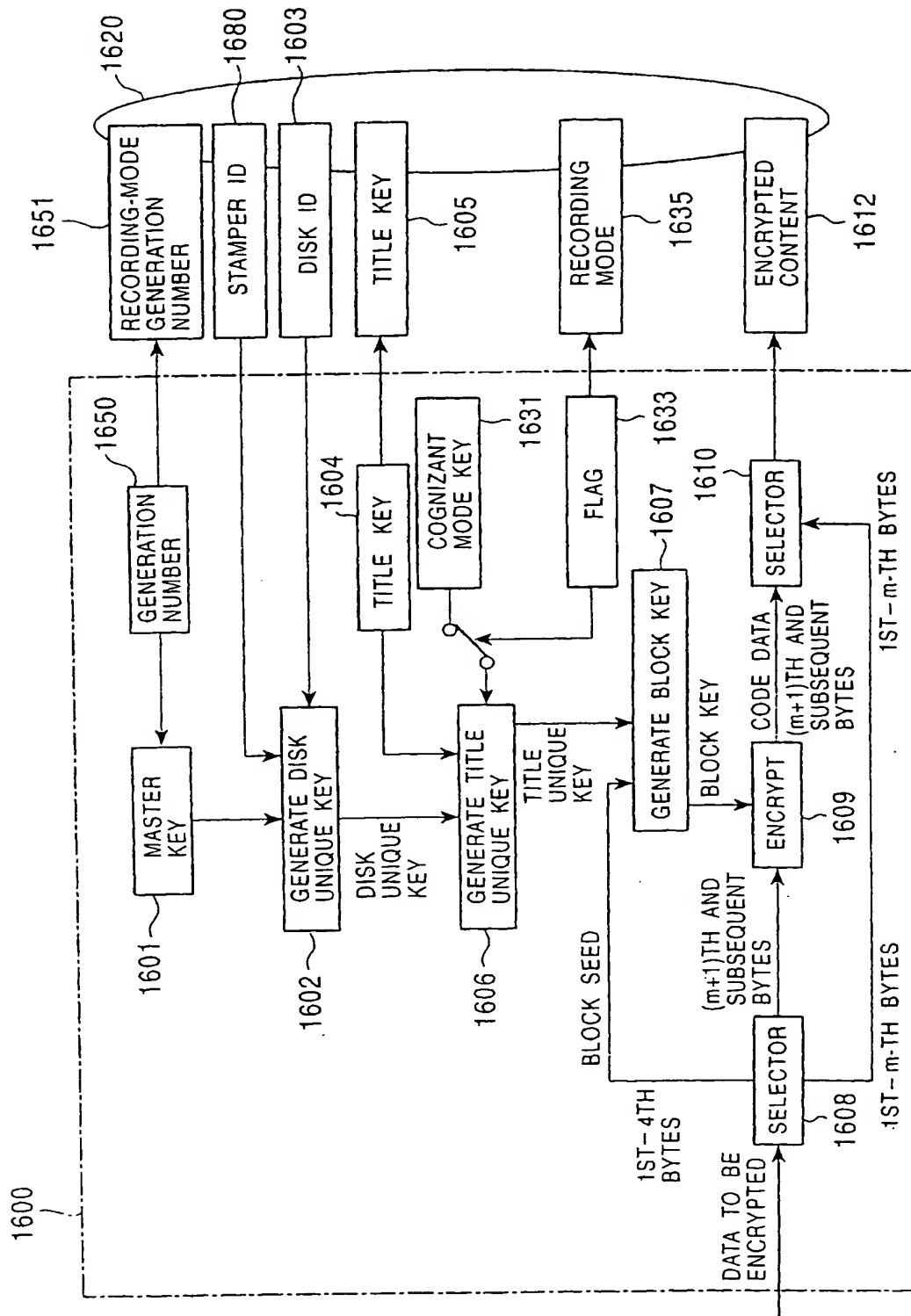


FIG. 30

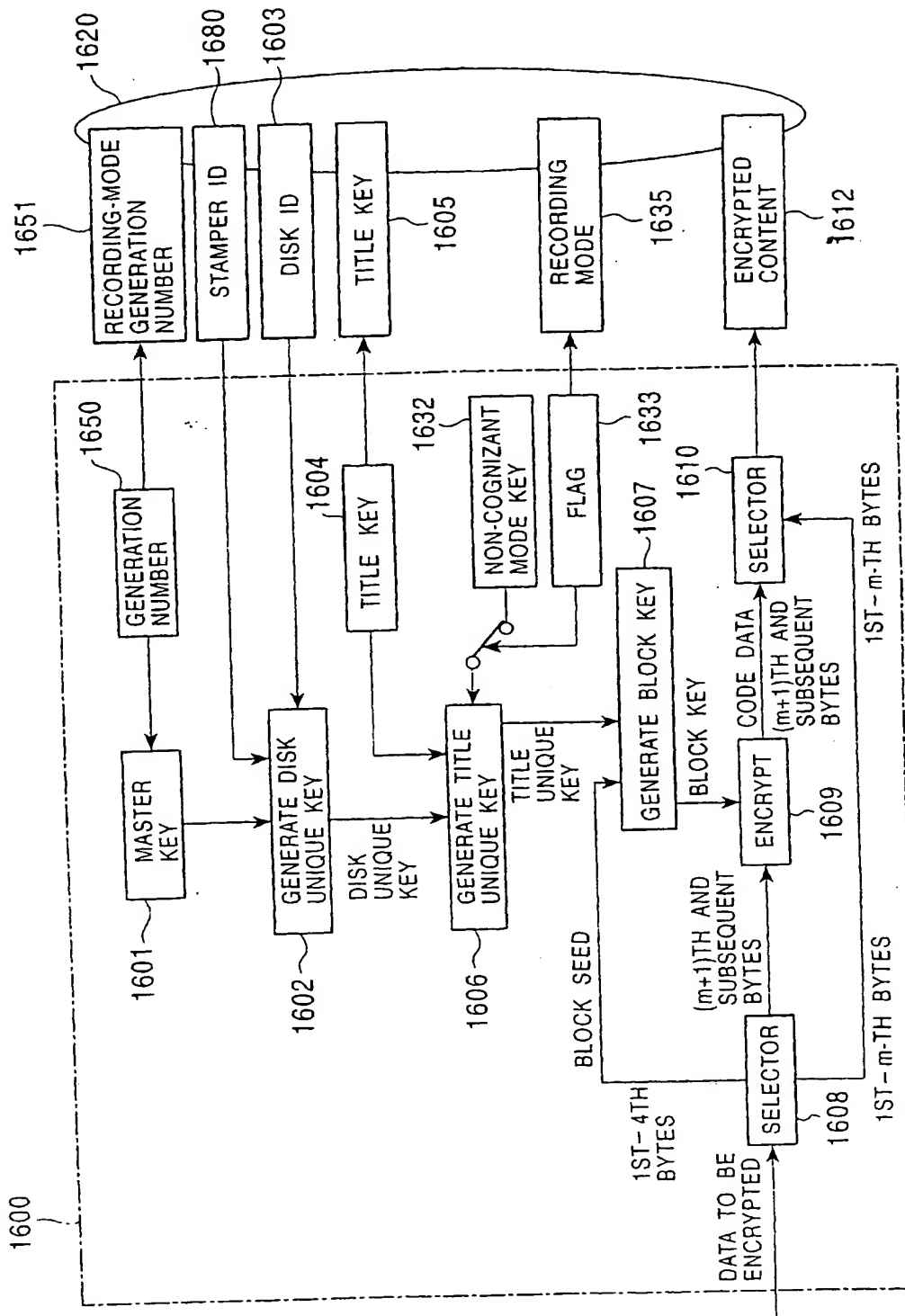


FIG. 31

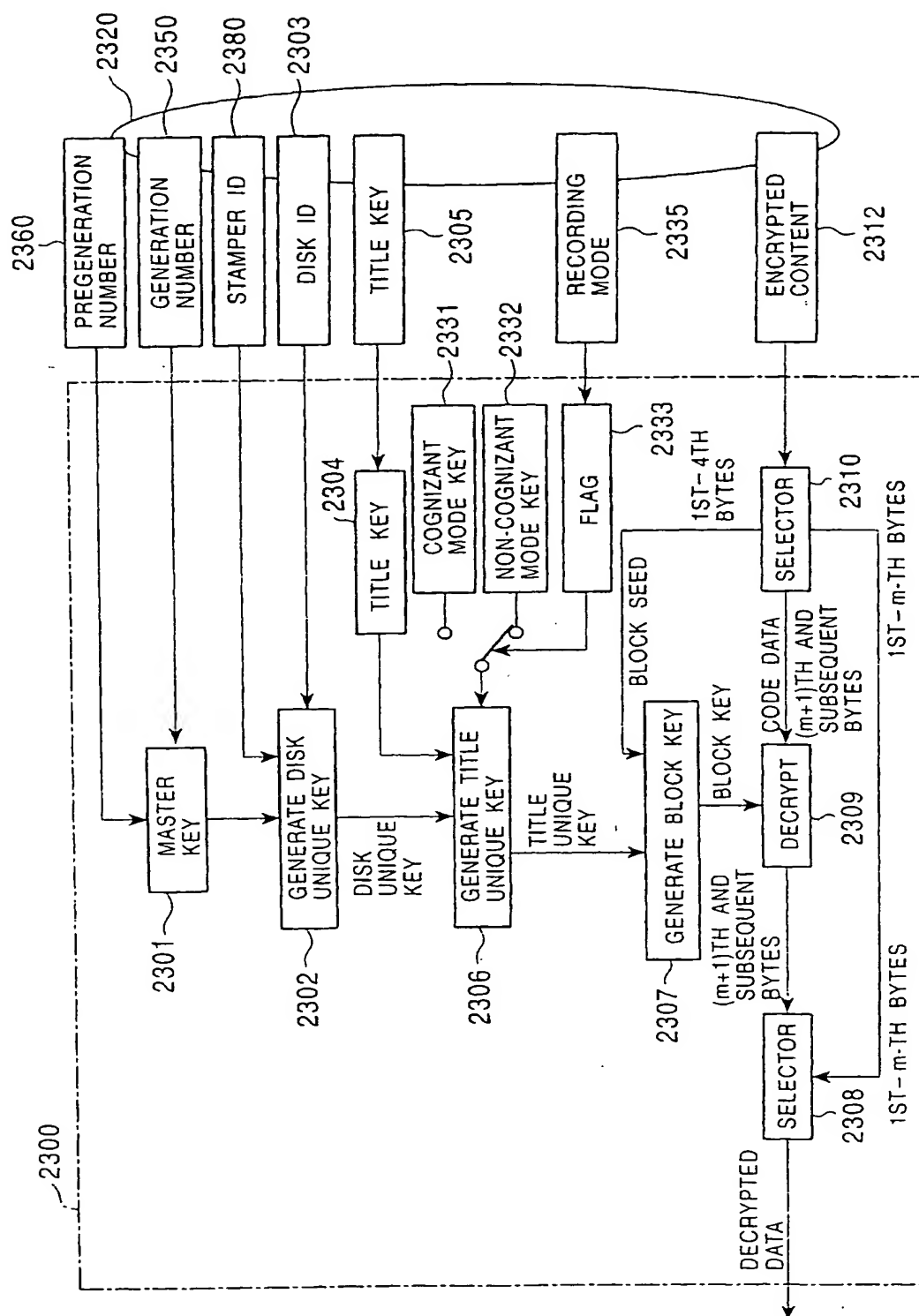


FIG. 32

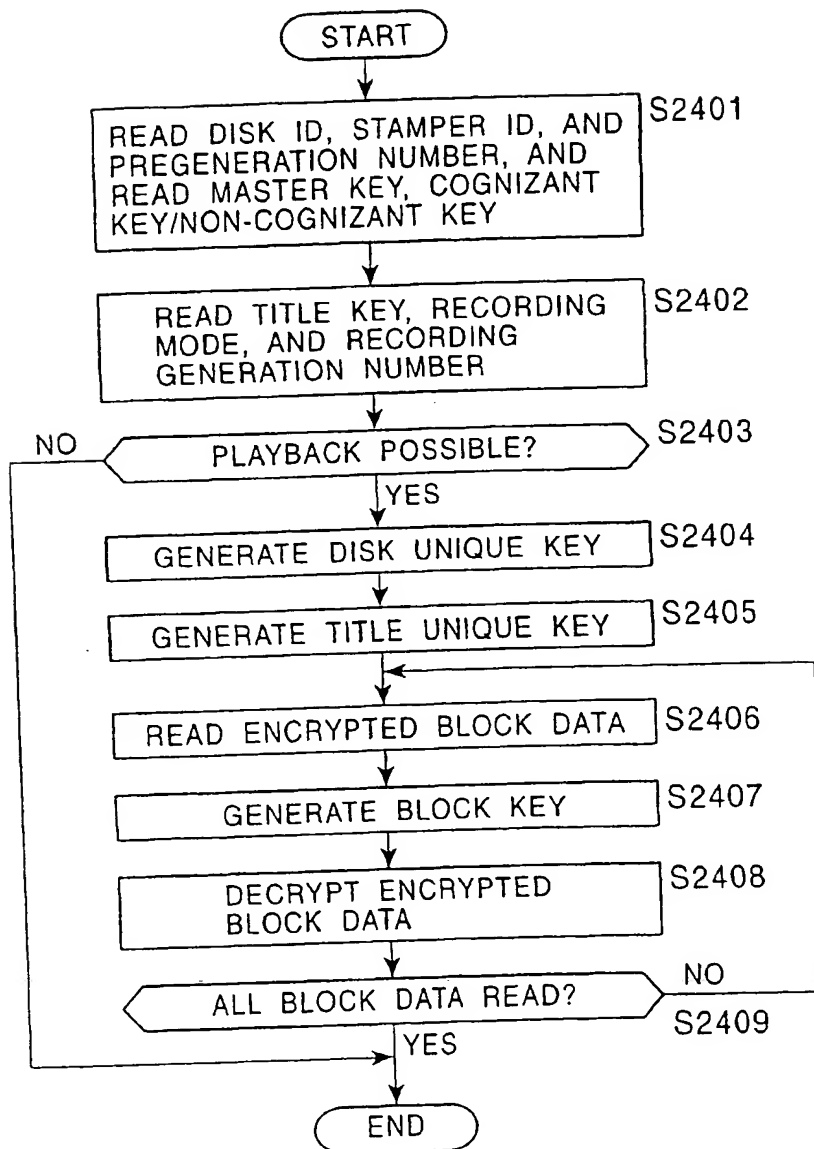


FIG. 33

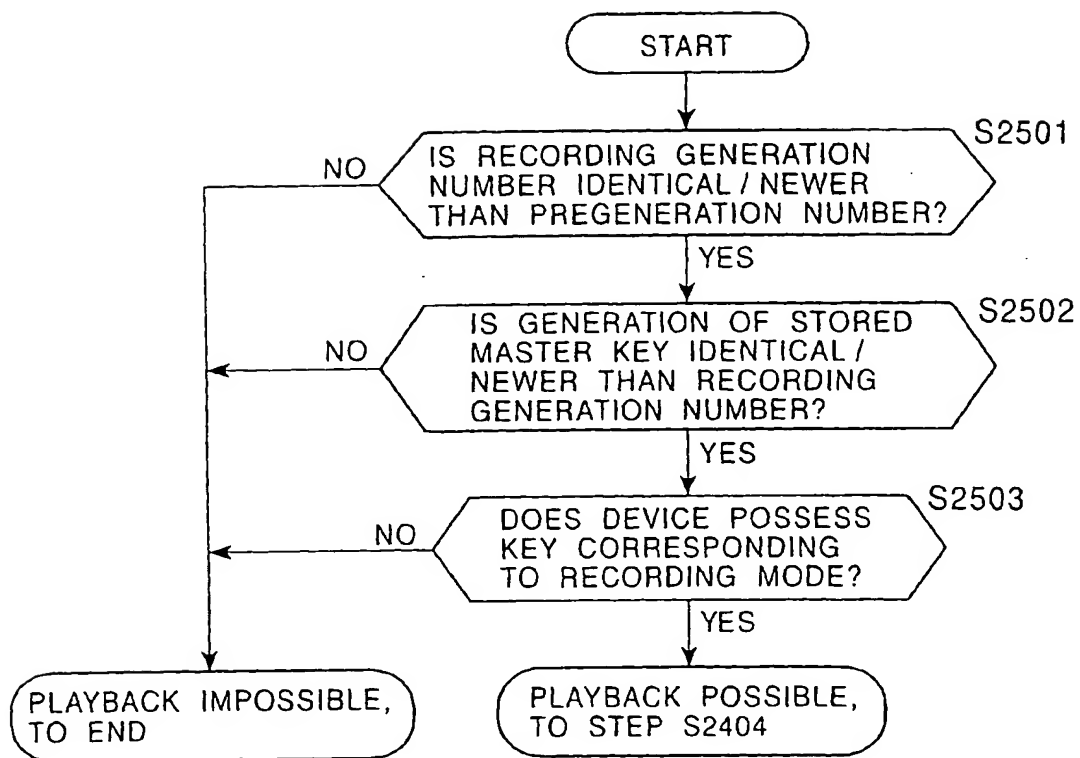


FIG. 34

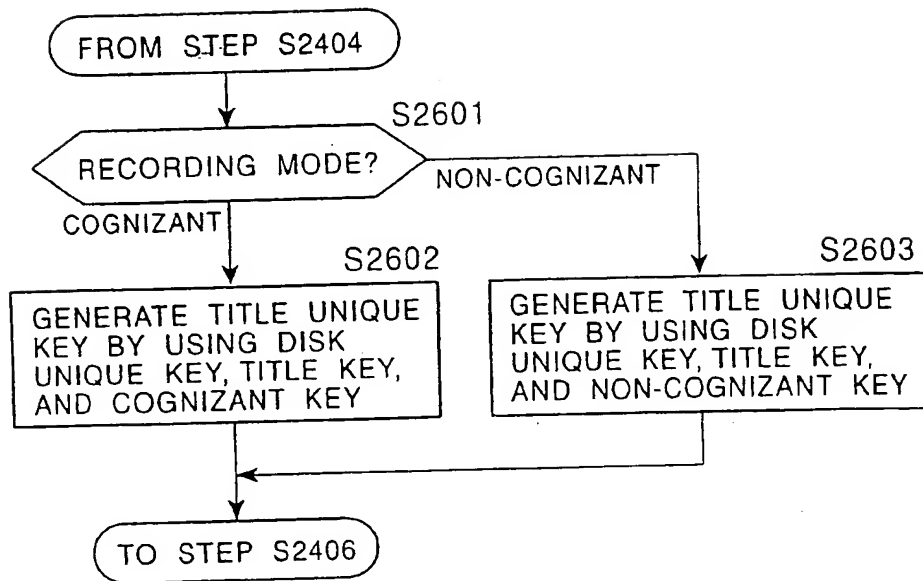


FIG. 35

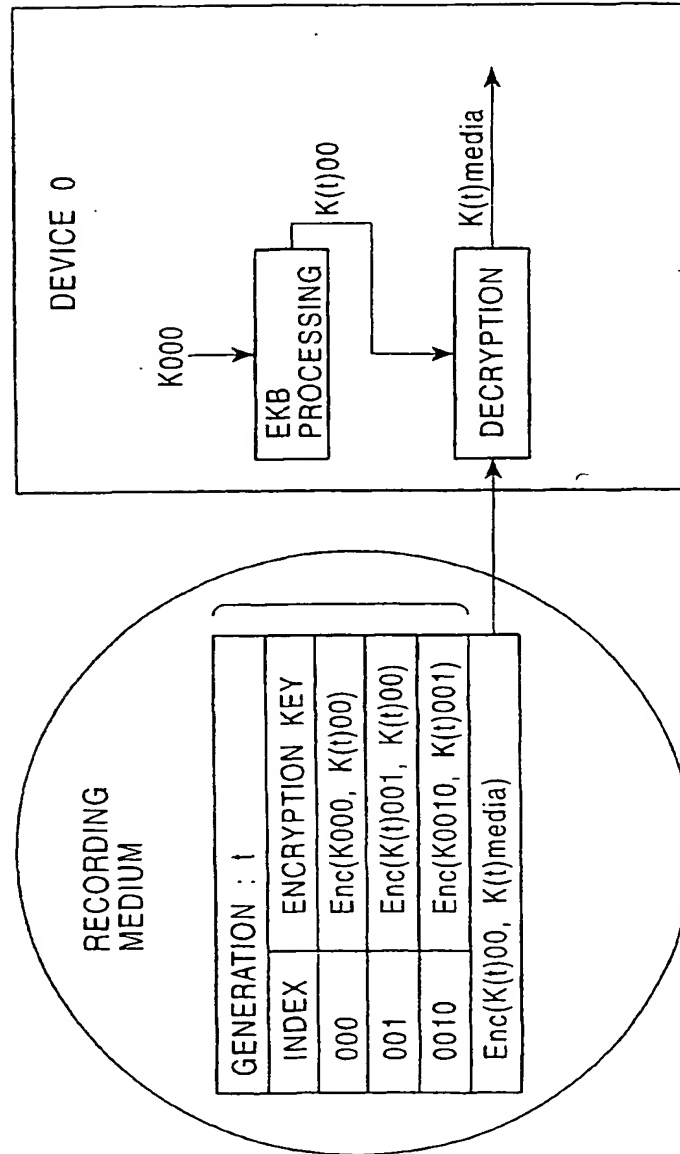


FIG. 36

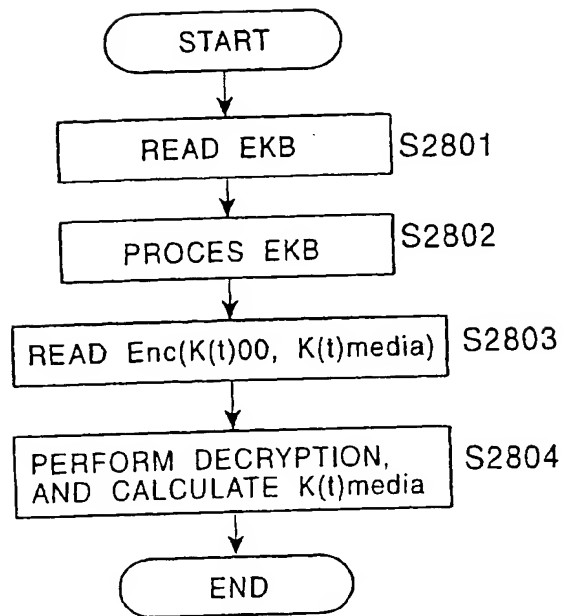


FIG. 37

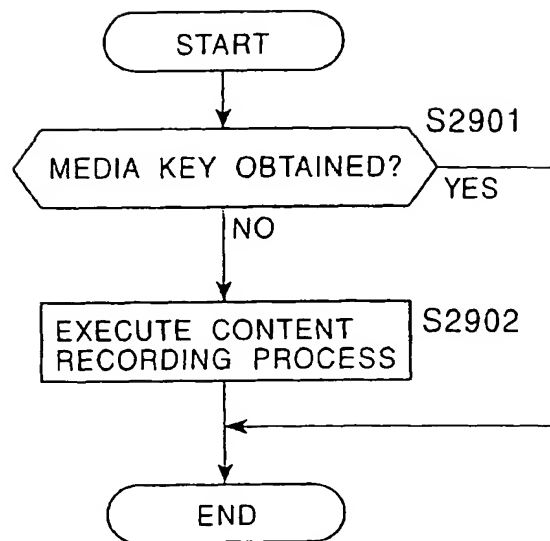


FIG. 38

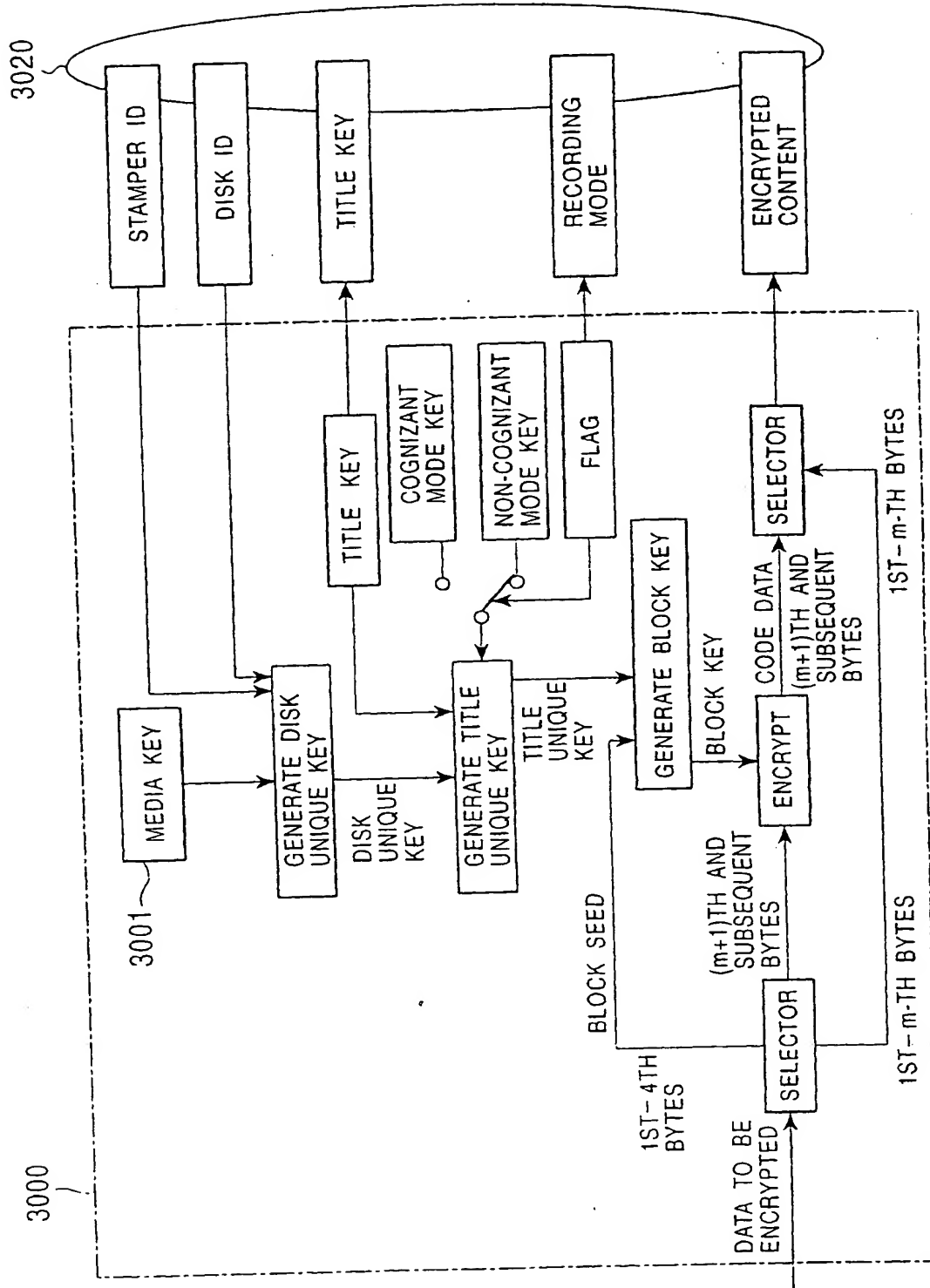


FIG. 39

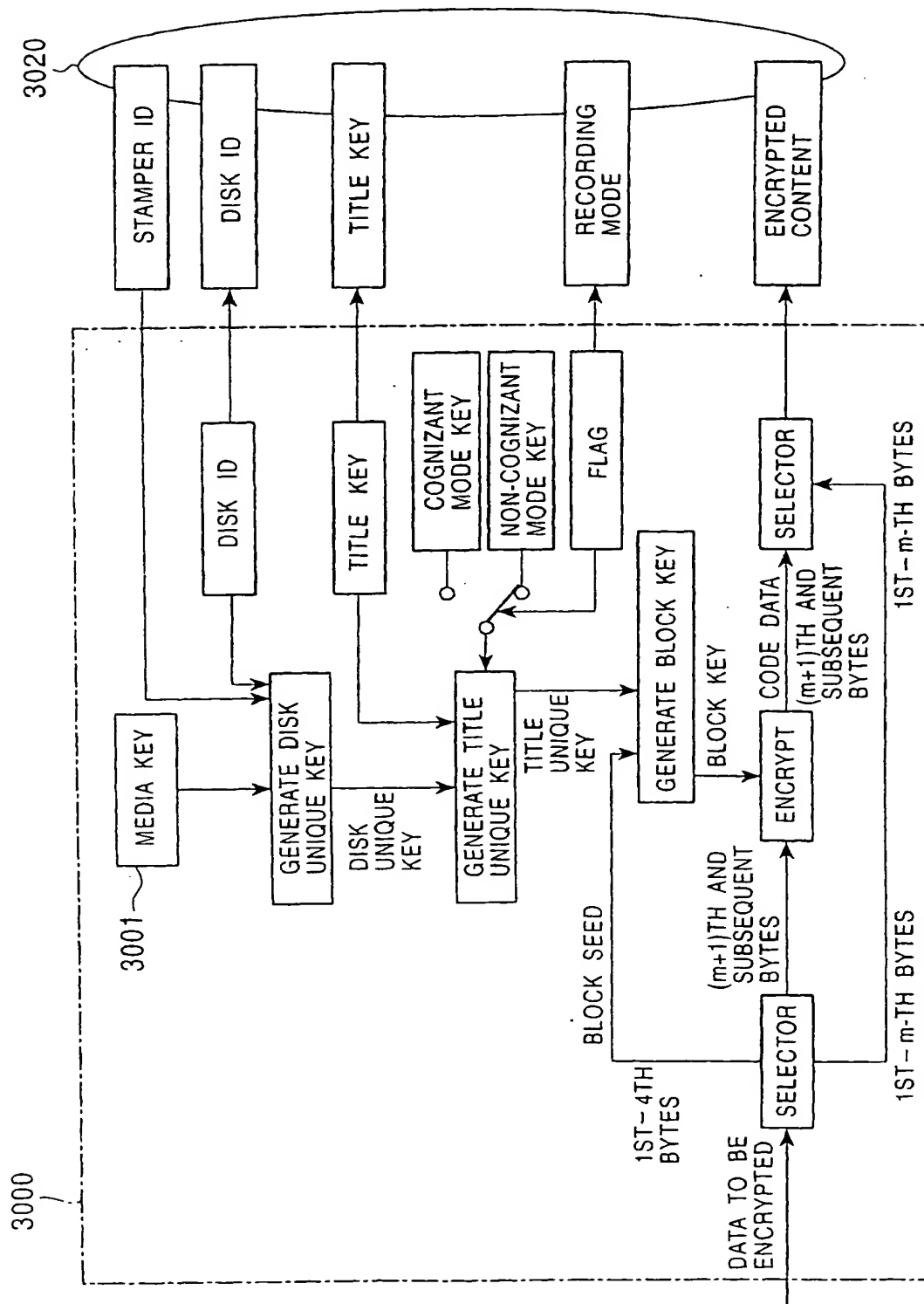


FIG. 40

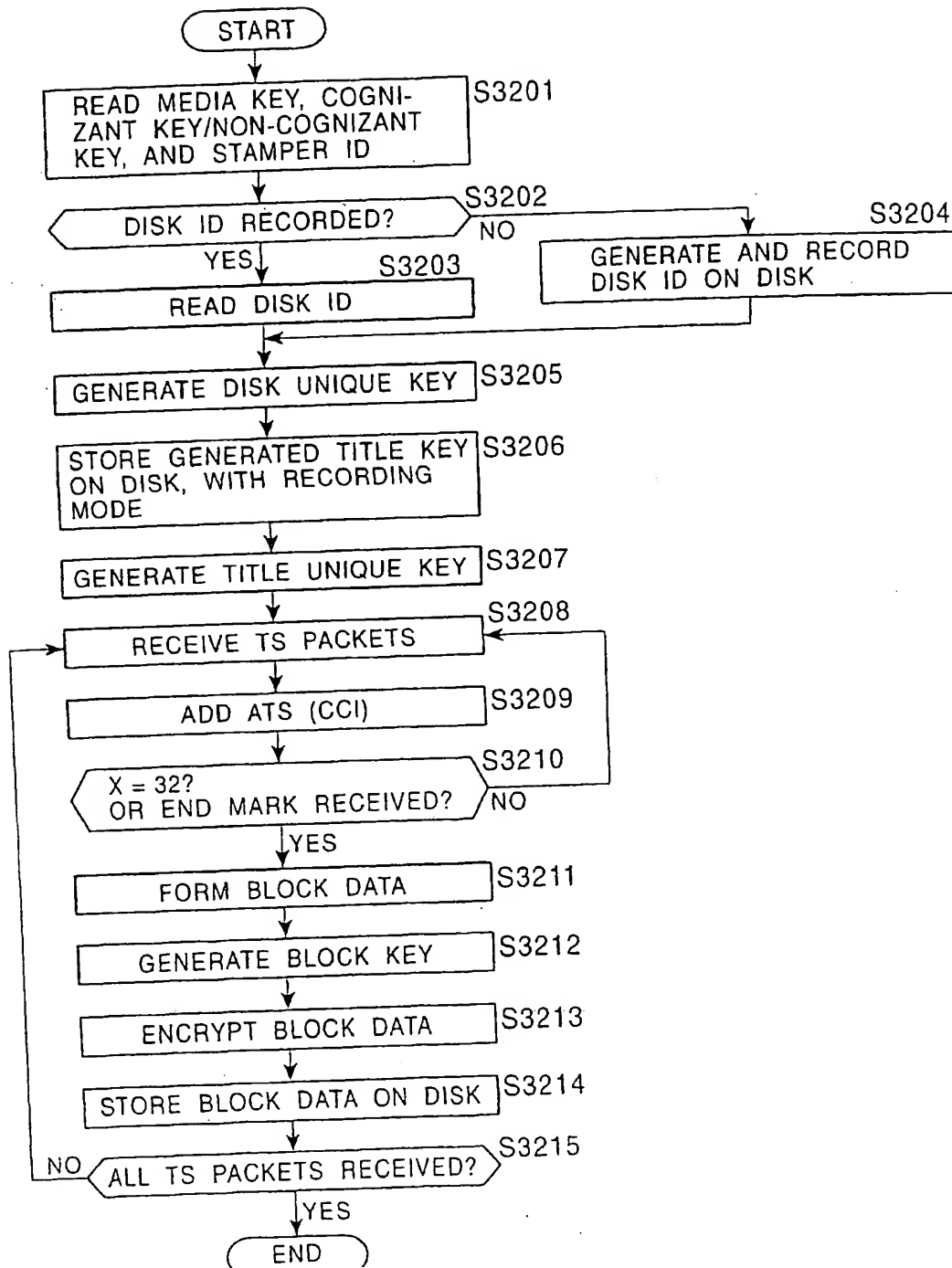


FIG. 41

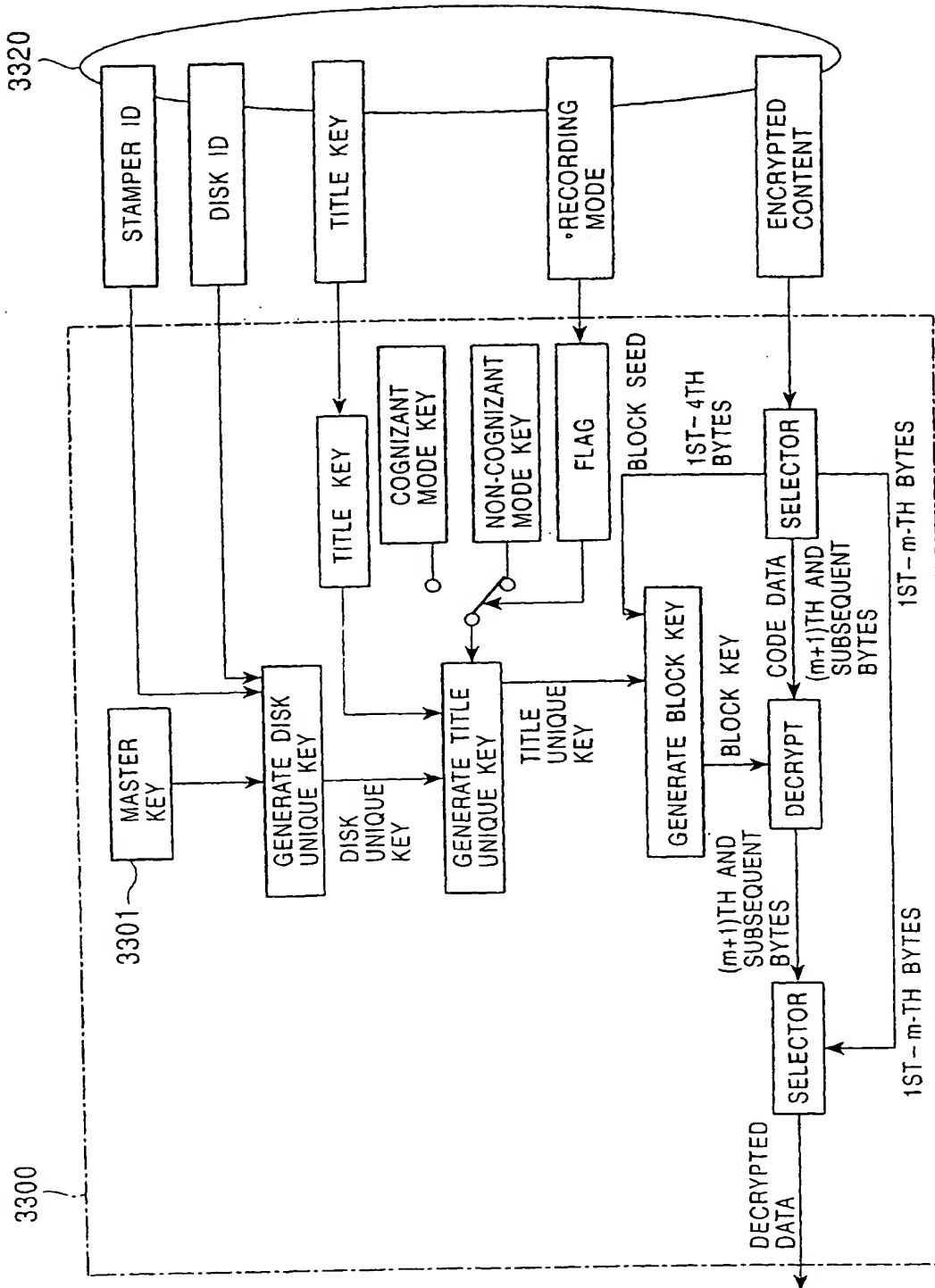


FIG. 42

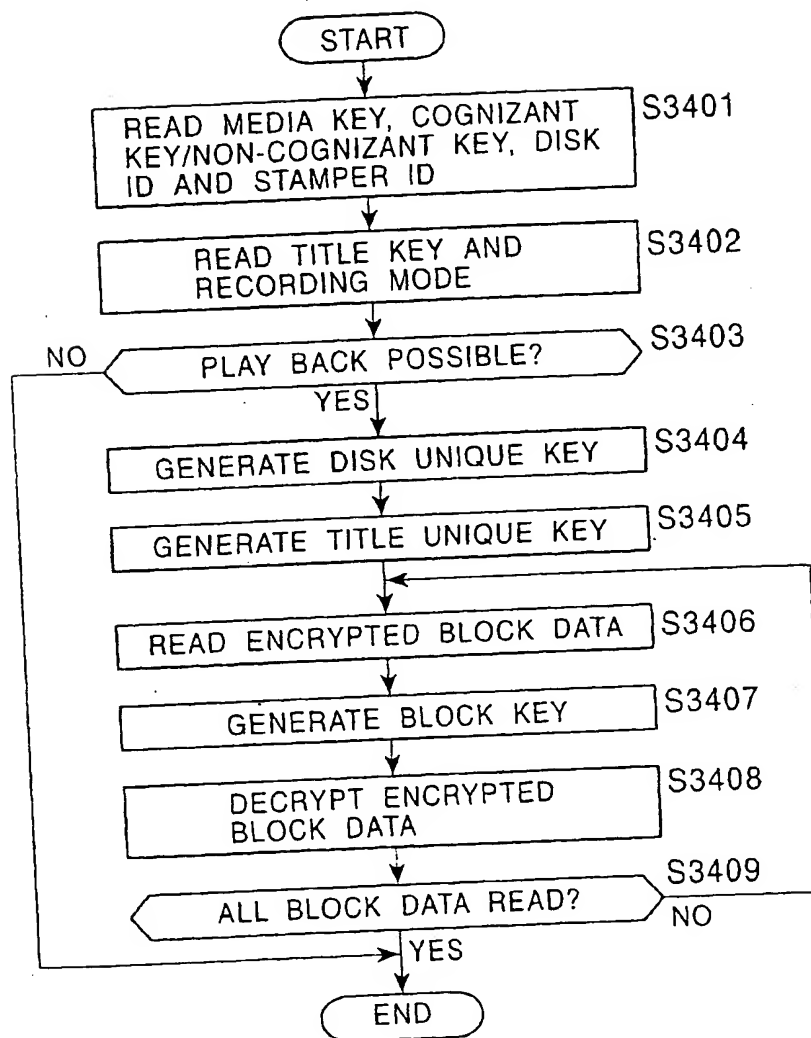


FIG. 43

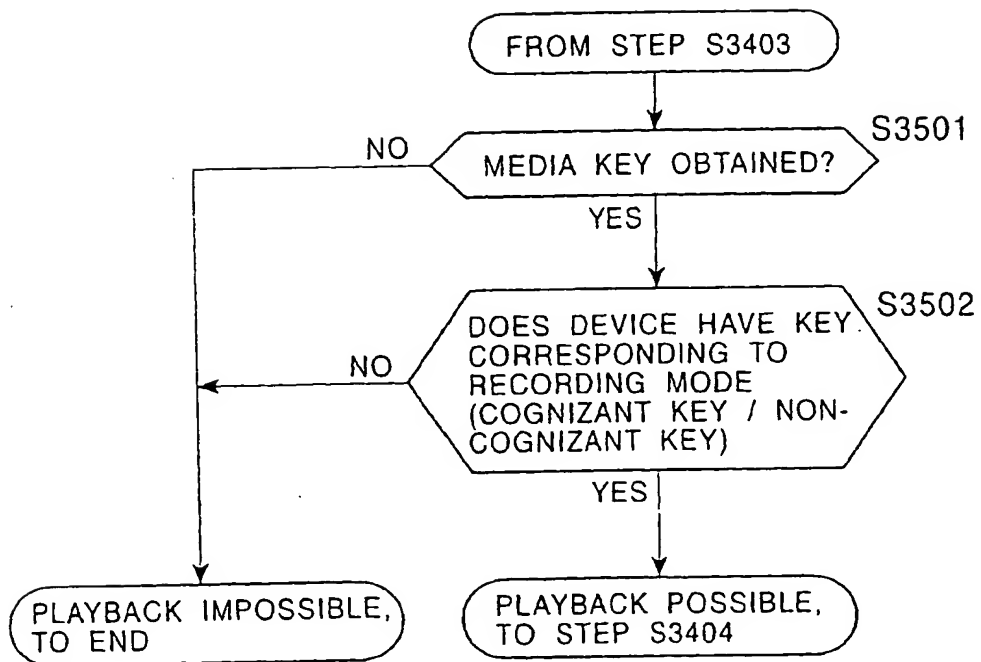


FIG. 44B

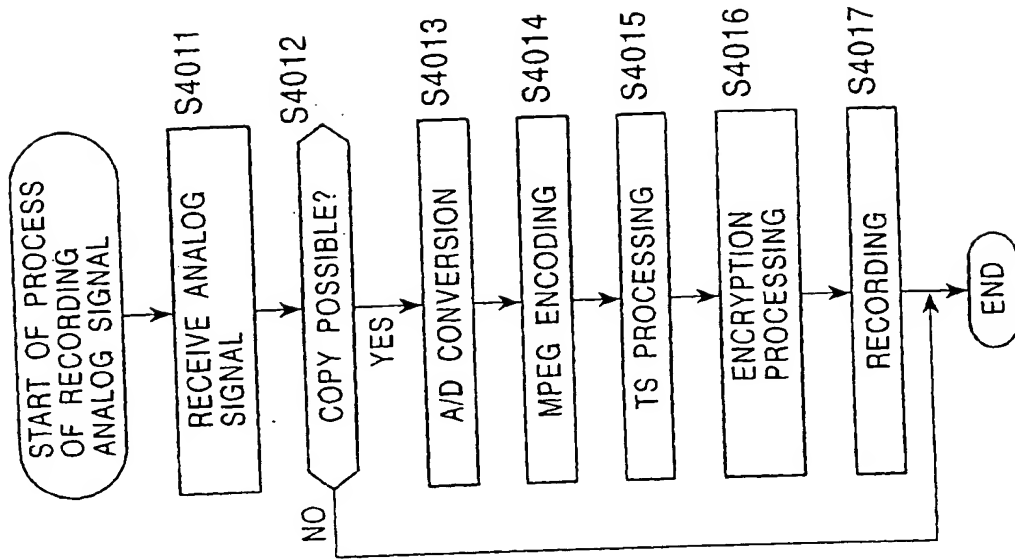


FIG. 44A

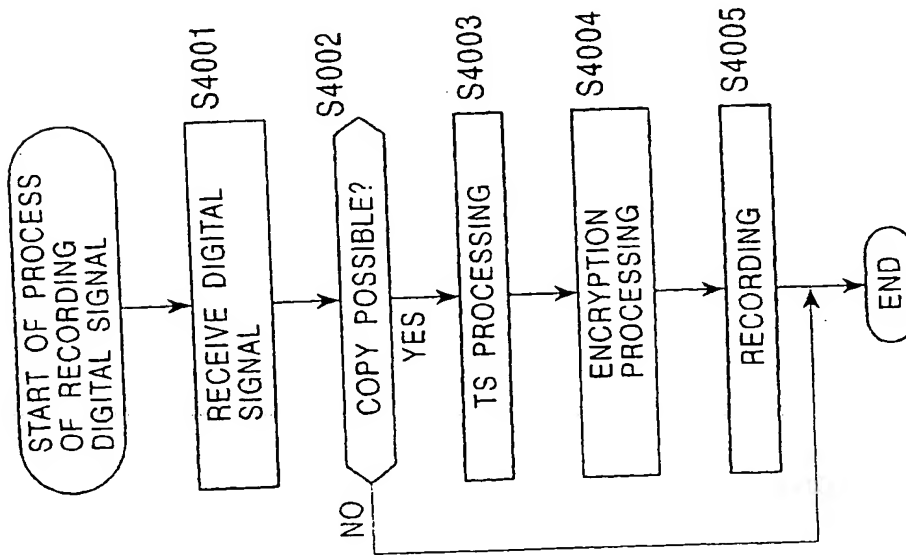


FIG. 45B

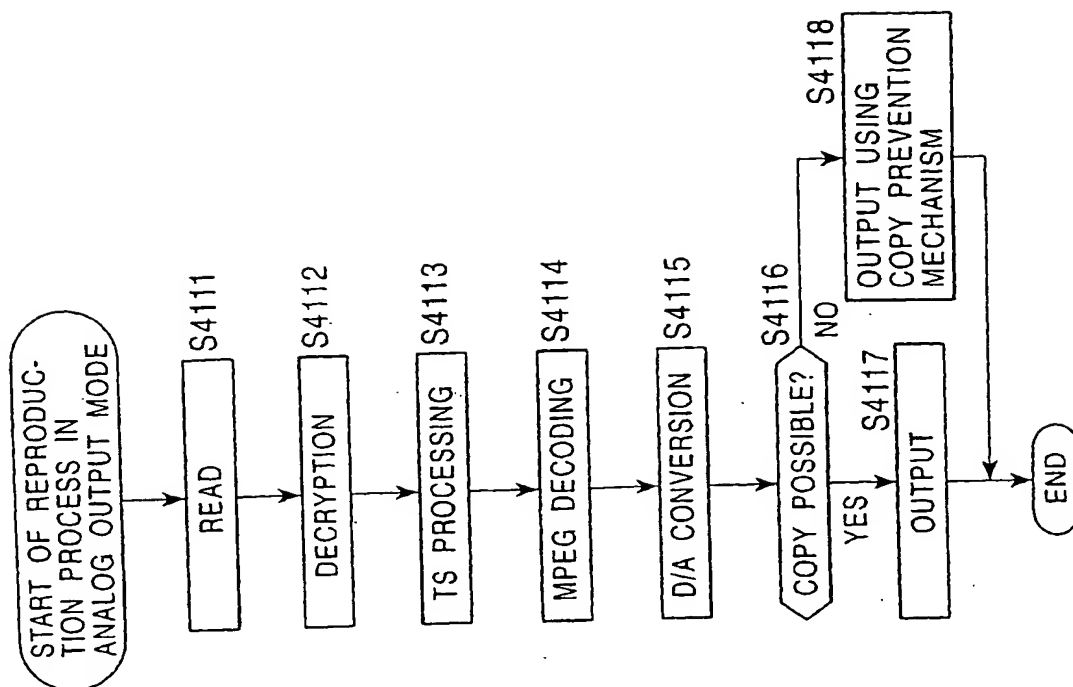


FIG. 45A

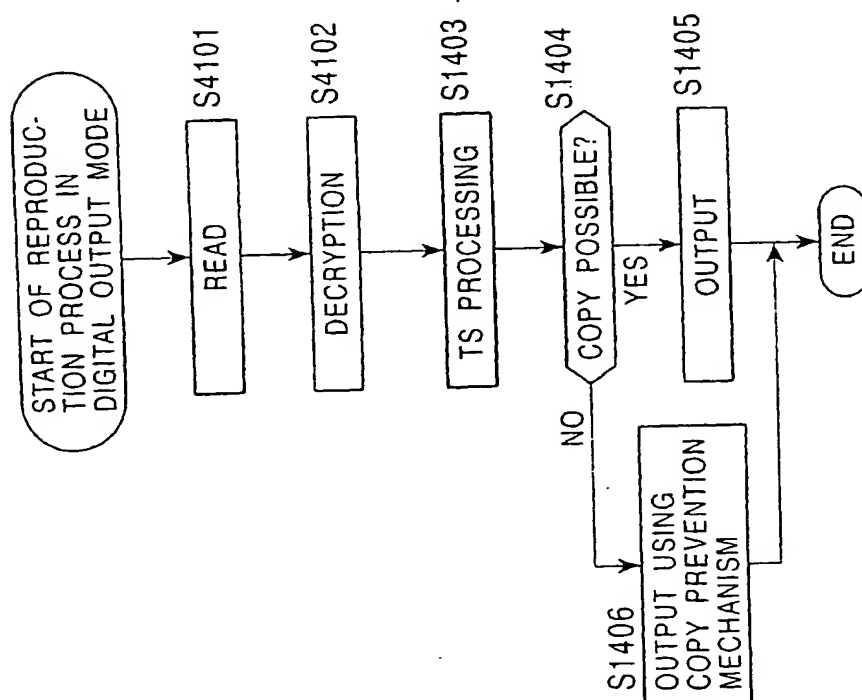


FIG. 46

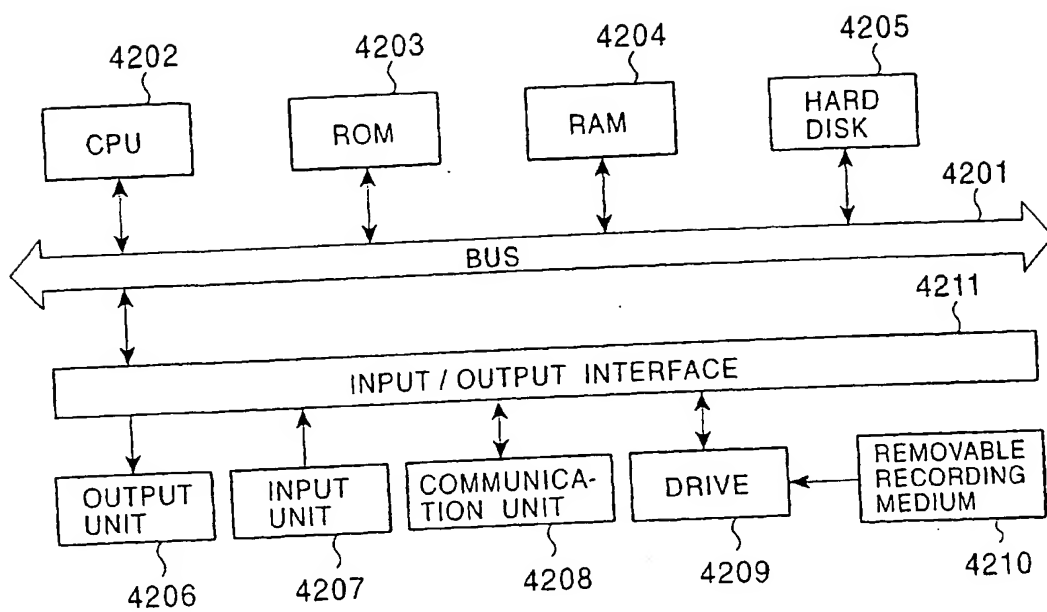


FIG. 47

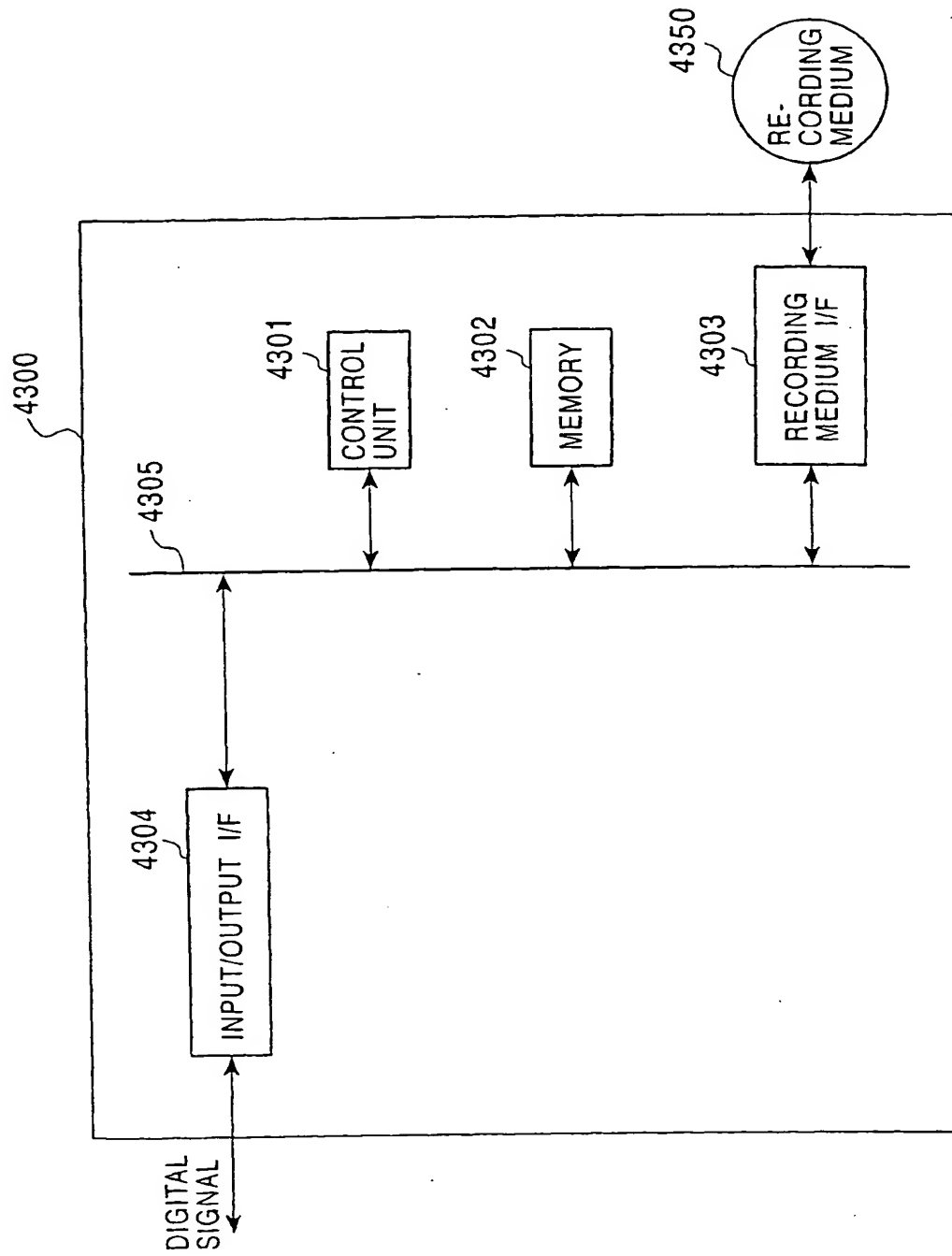


FIG. 48

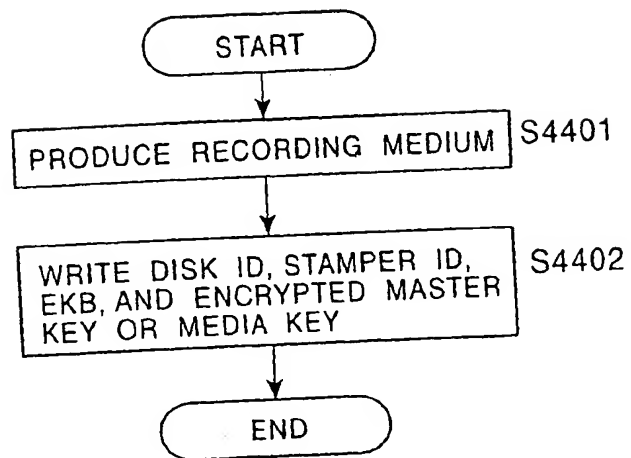


FIG. 49

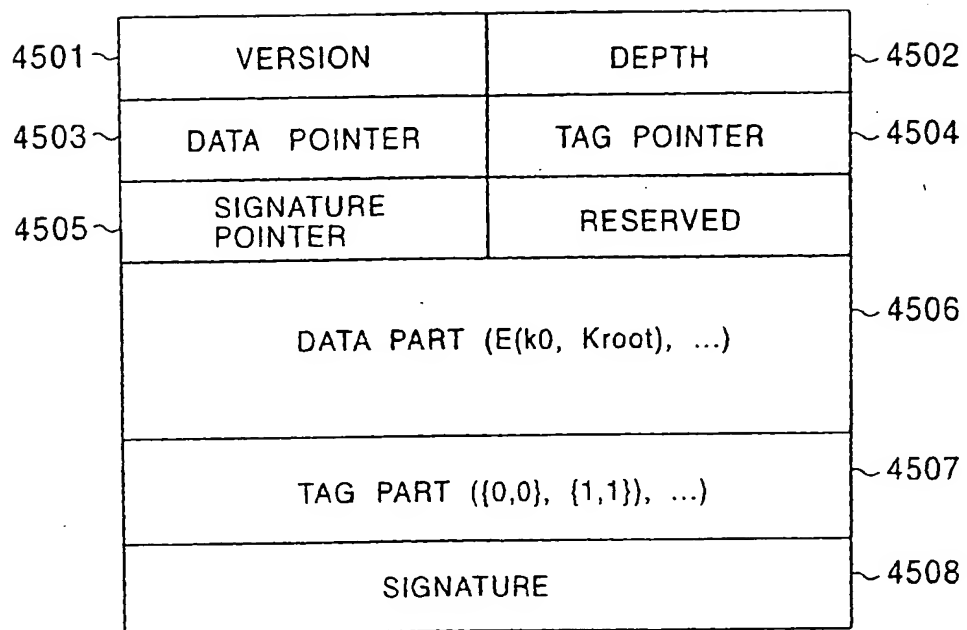


FIG. 50

